



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 1月12日

出 願 番 号

Application Number:

特願2001-005033

出 願 人

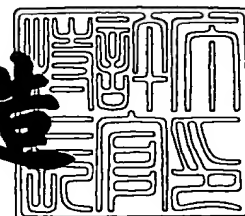
Applicant(s):

日本電信電話株式会社

2001年 6月13日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3055435

【書類名】 特許願

【整理番号】 NTTH126787

【提出日】 平成13年 1月12日

【あて先】 特許庁長官殿

【国際特許分類】 G07F 5/00  
G06K 9/00

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 重松 智志

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 斎藤 賢一

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 町田 克之

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 池田 奈美子

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 海野 秀之

【特許出願人】

    【識別番号】 000004226

    【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100064621  
【弁理士】  
【氏名又は名称】 山川 政樹  
【電話番号】 03-3580-0961

【手数料の表示】

【予納台帳番号】 006194  
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 9701512

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 生体情報認証保管庫及び施錠・解錠方法

【特許請求の範囲】

【請求項 1】 本体内部への物品の保管時及び前記本体内部に保管された物品の取り出し時にはそれぞれ前記本体の扉のロック及びロック解除が行われるとともに、利用者の生体情報の認証に基づいて前記扉のロックを解除する生体情報認証保管庫であって、

前記扉のロック及びロック解除を行う駆動手段と、

利用者の生体情報を記憶する記憶手段と、

利用者の生体情報を検出するセンサの検出情報と前記記憶手段の記憶情報との一致に基づき前記駆動手段を制御し前記扉のロックを解除させる処理手段とを備えたことを特徴とする生体情報認証保管庫。

【請求項 2】 請求項 1 において、

前記記憶手段には利用者の指紋画像が前記生体情報として記憶され、

前記処理手段は、利用者の指紋画像を前記生体情報として検出する前記センサを有する指紋認証トークンからの前記指紋画像と前記記憶手段の記憶情報との一致に基づき前記駆動手段を制御し前記扉のロックを解除させることを特徴とする生体情報認証保管庫。

【請求項 3】 請求項 2 において、

前記処理手段は、

本体内部への物品の保管時に指紋認証トークンから送信された利用者の指紋画像を受信すると前記駆動手段を制御して前記扉をロックさせかつ受信した指紋画像を記憶手段に記憶するロック手段と、

本体内部に保管された物品の取り出し時に指紋認証トークンから送信された利用者の指紋画像を受信するとこの受信指紋画像が記憶手段の記憶情報と一致する場合は前記駆動手段を制御し前記扉のロックを解除させるロック解除手段と

を有することを特徴とする生体情報認証保管庫。

【請求項 4】 請求項 2 において、

前記処理手段は、

本体内部への物品の保管時に指紋認証トークンが本体に差し込まれると前記駆動手段を制御して前記扉をロックさせ、かつパスワードを発生してこのパスワードを前記記憶手段に記憶するとともに、前記指紋認証トークンへ送信して記憶させるロック手段と、

本体内部に保管された物品の取り出し時に前記指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は前記駆動手段を制御し前記扉のロックを解除させるロック解除手段と

を有することを特徴とする生体情報認証保管庫。

【請求項 5】 請求項 2 において、

前記処理手段は、

本体内部への物品の保管時に指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、前記駆動手段を制御して前記扉をロックさせるとともに、受信したパスワードを前記記憶手段に記憶するロック手段と、

本体内部に保管された物品の取り出し時に前記指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は前記駆動手段を制御し前記扉のロックを解除させるロック解除手段と

を有することを特徴とする生体情報認証保管庫。

【請求項 6】 請求項 2 において、

それぞれ独立して物品の保管が可能な複数の保管部を設けるとともに、各保管部に対応して扉を設け、

複数の扉のうち何れかを指定する指定手段と、扉の番号を表示する表示手段とを有し、

前記処理手段は、

保管部への物品の保管時に対応の扉が閉じられるとこの扉の番号を表示手段に表示する第 1 の表示制御手段と、

表示手段に表示された扉の番号が前記指定手段により指定された後、指紋認証

トークンが本体に差し込まれると、前記駆動手段を制御して前記扉をロックさせ、かつパスワードを発生してこのパスワードと前記扉の番号とを前記記憶手段に記憶するとともに、前記指紋認証トークンへ送信して記憶させるロック手段と、

保管部に保管された物品の取り出し時に指紋認証トークンが本体に差し込まれると、この指紋認証トークンに記憶されている扉の番号を表示手段に表示する第2の表示制御手段と、

表示手段に表示された扉の番号が前記指定手段により指定された後、前記指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は前記駆動手段を制御し前記扉のロックを解除させるロック解除手段と

を有することを特徴とする生体情報認証保管庫。

【請求項7】 請求項1ないし請求項6の何れかの請求項において、

物品の保管時に利用者により投入された所定額のコインを確認する確認手段を設け、

前記処理手段は、前記確認手段により所定額のコインの投入が確認されると前記駆動手段を制御して前記扉をロックさせることを特徴とする生体情報認証保管庫。

【請求項8】 本体内部への物品の保管時及び前記本体内部に保管された物品の取り出し時にはそれぞれ前記本体の扉の施錠及び解錠が行われるとともに、利用者の生体情報の認証に基づいて前記扉の解錠を行う生体情報認証保管庫における施錠・解錠方法において、

利用者の生体情報を検出するセンサの検出情報と予め記憶手段に記憶されている記憶情報との一致に基づき前記扉を解錠する第1のステップを有することを特徴とする施錠・解錠方法。

【請求項9】 請求項8において、

前記記憶手段には利用者の指紋画像が前記生体情報として記憶され、

前記第1のステップにおける処理は、利用者の指紋画像を前記生体情報として検出する前記センサを有する指紋認証トークンからの前記指紋画像と前記記憶手

段の記憶情報との一致に基づき前記扉を解錠する第 2 のステップを含むことを特徴とする施錠・解錠方法。

【請求項 1 0】 請求項 9 において、

前記第 2 のステップにおける処理は、

本体内部への物品の保管時に前記指紋認証トークンから送信された利用者の指紋画像を受信すると前記扉を施錠しかつ受信した指紋画像を記憶手段に記憶する第 3 のステップと、

本体内部に保管された物品の取り出し時に前記指紋認証トークンから送信された利用者の指紋画像を受信するとこの受信指紋画像が記憶手段の記憶情報と一致する場合は前記扉を解錠する第 4 のステップと

を含むことを特徴とする施錠・解錠方法。

【請求項 1 1】 請求項 9 において、

前記第 2 のステップにおける処理は、

本体内部への物品の保管時に指紋認証トークンが本体に差し込まれると前記扉を施錠し、かつパスワードを発生してこのパスワードを前記記憶手段に記憶するとともに、前記指紋認証トークンへ送信して記憶させる第 5 のステップと、

本体内部に保管された物品の取り出し時に前記指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は前記扉を解錠する第 6 のステップと

を含むことを特徴とする施錠・解錠方法。

【請求項 1 2】 請求項 9 において、

前記第 2 のステップにおける処理は、

本体内部への物品の保管時に指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、前記扉を施錠するとともに、受信したパスワードを前記記憶手段に記憶する第 7 のステップと、

本体内部に保管された物品の取り出し時に前記指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを

受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は前記扉を解錠する第 8 のステップと

を含むことを特徴とする施錠・解錠方法。

【請求項 1 3】 請求項 9 において、

それぞれ独立して物品の保管が可能な複数の保管部を設けるとともに、各保管部に対応して扉を設け、

前記第 2 のステップにおける処理は、

保管部への物品の保管時に対応の扉が閉じられるとこの扉の番号を表示する第 9 のステップと、

第 9 のステップの処理に基づき表示された扉の番号が指定された後、指紋認証トークンが本体に差し込まれると前記扉を施錠し、かつパスワードを発生してこのパスワードと前記扉の番号とを前記記憶手段に記憶するとともに、前記指紋認証トークンへ送信して記憶させる第 1 0 のステップと、

保管部に保管された物品の取り出し時に指紋認証トークンが本体に差し込まれると、この指紋認証トークンに記憶されている扉の番号を表示する第 1 1 のステップと、

第 1 1 のステップの処理に基づき表示された扉の番号が指定された後、前記指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は前記扉を解錠する第 1 2 のステップと

を含むことを特徴とする施錠・解錠方法。

【請求項 1 4】 請求項 8 ないし請求項 1 3 の何れかの請求項において、

物品の保管時に利用者により投入された所定額のコインを確認する第 1 3 のステップを有し、

前記第 1 のステップにおける処理は、前記第 1 3 のステップの処理に基づき所定額のコインの投入が確認されると前記扉を施錠する第 1 4 のステップを含むことを特徴とする施錠・解錠方法。

【発明の詳細な説明】

【0 0 0 1】



【発明の属する技術分野】

本発明は、物品を保管するとともに指紋等の生体情報の認証に基づき扉のロック及びロック解除を行う生体情報認証保管庫及び施錠・解錠方法に関する。

【0002】

【従来の技術】

コインの投入に基づき内部に物品の保管が可能なコインロッカーには、鍵が付与されている。利用者がこのようなコインロッカーを使用して内部に自身の物品を保管する場合は、利用者は前述の鍵により扉を解錠した後、扉を開けて内部に物品を収納する。その後、コイン投入口にコインを投入して扉を閉め、前述の鍵により扉の施錠を行うようにしている。

【0003】

【発明が解決しようとする課題】

利用者はコインロッカーに自身の物品を保管すると、そのコインロッカーの鍵を所持しているが、鍵を紛失するとその鍵を利用した第三者により容易にそのコインロッカーが解錠され、内部に保管されている貴重品等が盗難されるという問題があった。

したがって、本発明は、コインロッカー等の物品保管庫において、第三者による保管庫の解錠を阻止しセキュリティを確保することを目的とする。

【0004】

【課題を解決するための手段】

このような課題を解決するために本発明は、本体内部への物品の保管時及び本体内部に保管された物品の取り出し時にはそれぞれ本体の扉のロック及びロック解除が行われるとともに、生体情報の認証に基づいて扉のロックを解除する生体情報認証保管庫であって、扉のロック及びロック解除を行う駆動手段と、利用者の生体情報を記憶する記憶手段と、利用者の生体情報を検出するセンサの検出情報と記憶手段の記憶情報との一致に基づき駆動手段を制御し扉のロックを解除させる処理手段とを設けたものである。

【0005】

この場合、生体情報としては、利用者の指の大きさ、手形、静脈パターン、人

相、虹彩、声紋、利用者のサイン（筆跡）等の利用者固有の情報を用いることができるが、本発明の一構成例は、記憶手段には利用者の指紋画像を生体情報として記憶し、処理手段は、利用者の指紋画像を生体情報として検出する前記センサを有する指紋認証トークンからの指紋画像と記憶手段の記憶情報との一致に基づき駆動手段を制御し扉のロックを解除させるものである。

また、処理手段は、本体内部への物品の保管時に指紋認証トークンから送信された利用者の指紋画像を受信すると扉をロックし、かつ受信した指紋画像を記憶手段に記憶するロック手段と、本体内部に保管された物品の取り出し時に指紋認証トークンから送信された利用者の指紋画像を受信するとこの受信指紋画像が記憶手段の記憶情報と一致する場合は扉のロックを解除するロック解除手段とを有するものである。

【 0 0 0 6 】

また、処理手段は、本体内部への物品の保管時に指紋認証トークンが本体に差し込まれると扉をロックし、かつパスワードを発生してこのパスワードを記憶手段に記憶するとともに、指紋認証トークンへ送信して記憶させるロック手段と、本体内部に保管された物品の取り出し時に指紋認証トークンから出力される前記センサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は扉のロックを解除するロック解除手段とを有するものである。

また、処理手段は、本体内部への物品の保管時に指紋認証トークンから出力されるセンサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると扉をロックするとともに、受信したパスワードを記憶手段に記憶するロック手段と、本体内部に保管された物品の取り出し時に指紋認証トークンから出力されるセンサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は扉のロックを解除するロック解除手段とを有するものである。

【 0 0 0 7 】

また、それぞれ独立して物品の保管が可能な複数の保管部を設けるとともに、各保管部に対応して扉を設け、かつ複数の扉のうち何れかを指定する指定手段と

、扉の番号を表示する表示手段とを設け、処理手段は、保管部への物品の保管時に対応の扉が閉じられるとこの扉の番号を表示手段に表示する第 1 の表示制御手段と、表示された扉の番号が指定手段により指定された後、指紋認証トークンが本体に差し込まれると扉をロックし、かつパスワードを発生してこのパスワードと扉の番号とを記憶手段に記憶するとともに、指紋認証トークンへ送信して記憶させるロック手段と、保管部に保管された物品の取り出し時に指紋認証トークンが本体に差し込まれると、この指紋認証トークンに記憶されている扉の番号を表示手段に表示する第 2 の表示制御手段と、表示された扉の番号が指定手段により指定された後、指紋認証トークンから出力されるセンサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は扉のロックを解除するロック解除手段とを有するものである。

さらに、物品の保管時に利用者により投入された所定額のコインを確認する確認手段を設け、処理手段は、確認手段により所定額のコインの投入が確認されると扉をロックするようにしたものである。

【 0 0 0 8 】

【発明の実施の形態】

以下、本発明について図面を参照して説明する。

図 1 は、本発明に係る生体情報認証保管庫の外観を示す図であり、この生体情報認証保管庫は指紋認証保管庫であって、指紋認証保管庫 1 0 0 の本体 1 0 0 A には扉 1 0 1 が設けられているとともに、コインが投入されるコイン投入口 1 0 2 及び後述の指紋認証トークンが差し込まれる差込口 1 0 3 が設けられ、本体 1 0 0 A の内部に物品の保管ができるものである。

【 0 0 0 9 】

この指紋認証保管庫 1 0 0 の前記差込口 1 0 3 に差し込まれる指紋認証トークンは、利用者が所持し、持ち運びのできる小型、軽量の装置であって、図 2 に示すように、本体部 2 0 1 が設けられているとともに、本体部 2 0 1 に、指紋センサ 2 0 2 と、処理装置 2 0 3 と、記憶装置 2 0 4 と、指紋認証保管庫 1 0 0 との接続端子である端子 2 0 5 とが設けられている。そして、処理装置 2 0 3 は、指

紋センサ202, 記憶装置204及び端子205に接続されている。

【0010】

また、前記指紋認証保管庫100の本体100Aには、図3に示すように、コイン投入口102に投入されたコインを検出して所定の処理を行うとともに、差込口103に指紋認証トークン200が差し込まれるとその指紋認証トークン200からの指紋情報の認証処理等を行う処理装置111と、処理装置111に接続される記憶装置112と、処理装置111に接続され処理装置111の制御に基づき扉101の解錠及び施錠を行う錠制御装置113とが設けられている。

【0011】

図9は前記指紋認証トークン200を構成する指紋センサ202の概略的な断面を示す図である。本指紋センサ202は、例えばシリコンからなる半導体基板211上の下層絶縁膜212上に形成された層間絶縁膜214上に、たとえば80 $\mu$ m角の複数のセンサ電極215と、格子状のアース電極216とを備え、複数のセンサ電極215とアース電極216とを、層間絶縁膜214表面で規定される同一平面上に配置している。

【0012】

センサ電極215は、層間絶縁膜214上に形成されたパシベーション膜217で覆い、150 $\mu$ m間隔に複数個を備えるようにするとともに、Auから構成し、膜厚1 $\mu$ m程度に形成している。パシベーション膜217の膜厚は3 $\mu$ m程度としたので、センサ電極215上には、パシベーション膜217が約2(=3-1) $\mu$ m存在している。このパシベーション膜217は、例えばポリイミドなどの比誘電率が4.0程度の絶縁物から構成される。

【0013】

上記下層絶縁膜212上には、センサ電極215にスルーホールを介して接続する配線213を形成する一方、半導体基板211上には、センサ電極215に形成される容量を検出する容量検出回路218を形成している。この容量検出回路218は、前述した配線213によってセンサ電極215に接続される。容量検出回路218は、センサ電極215毎に用意され、センサ電極215と認識対象(指)の一部との間に形成される容量を検出する。

## 【0014】

各容量検出回路218の出力は、処理装置203に接続され、この処理装置203により、各センサ電極215に形成された容量を濃淡に変換した指紋画像データが生成される。

各容量検出回路218、処理装置203及び記憶装置204は、たとえばセンサ電極215下の半導体基板211上に形成する。これにより指紋センサ202、処理装置203及び記憶装置204をワンチップ化でき、したがって指紋認証トークン200のワンチップ化が可能になる。なお、こうしたワンチップ化の他の例として、例えば特開2000-242771に開示されたものがある。

## 【0015】

図10は図9に示す容量検出回路218の具体的な構成を示す回路図である。図10において、センサ電極215は、NチャネルMOSトランジスタQ2を介し、電流Iの電流源232aの入力側に接続されている。また、センサ電極215とトランジスタQ2との節点N1には、出力回路233の入力側が接続されている。また、節点N1には、PチャネルMOSトランジスタQ1を介して電源電圧VDDが印加される。この節点N1は、寄生容量Cp0を有している。

## 【0016】

さらに、トランジスタQ1、Q2のゲート端子には、各々信号PRE（バー）、REが印加される。ここで、電流源232aとトランジスタQ2とにより信号発生回路232が構成され、NチャネルMOSトランジスタQ3とバイアス抵抗Raとにより出力回路233が構成される。上記トランジスタなどの素子は、図7に示した下層絶縁膜212下の半導体基板211上に形成されている。また、上記各トランジスタなどの素子は、例えば、下層絶縁膜212上の配線層により接続され、上記回路を構成している。

## 【0017】

次に容量検出回路218の動作について説明する。

はじめに、トランジスタQ1のゲート端子には「High」レベル（VDD）の信号PRE（バー）が与えられ、トランジスタQ2のゲート端子には「Low」レベル（GND）の信号REが与えられている。したがって、このときトランジ

スタQ1, Q2はともに導通していない。

この状態で信号PRE (バー) が、「High」レベルから「Low」レベルに変化すると、トランジスタQ1が導通状態になる。このときトランジスタQ2は、非導通状態のままであるため節点N1の電位がVDDにプリチャージされる。

#### 【0018】

プリチャージが終了した後、信号PRE (バー) が、「High」レベルに変化すると同時に信号REが、「High」レベルに変化する。これにより、トランジスタQ1が非導通状態に、かつトランジスタQ2が導通状態になり、電流源232aにより節点N1の充電電荷が引き抜かれる。この結果、節点N1の電位が低下する。

信号REを「High」レベルにする期間を $\Delta t$ とすると、 $\Delta t$ 経過後の節点N1の電位低下 $\Delta V$ は、

$$\Delta V = I \Delta t / (C_f + C_{p0}) \cdots (1) \text{ となる。}$$

ただし、(1)式において、 $C_f$ はセンサ電極215と検出対象である指の表面230との間の容量値である。

#### 【0019】

電流源232aの電流 $I$ と期間 $\Delta t$ と寄生容量 $C_{p0}$ は、各々一定であるから、電位低下 $\Delta V$ は、センサ電極215と検出対象である指の表面230との間に発生する容量の値 $C_f$ によって決定される。この容量値 $C_f$ は、センサ電極215と指の表面230との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位 $\Delta V$ の大きさが、指紋の凹凸を反映して変化する。この電位低下 $\Delta V$ が、入力信号として出力回路233に供給されるので、出力回路233で $\Delta V$ が入力され、指紋の凹凸を反映した信号が出力される。

こうした各容量検出回路218の出力信号が処理装置203により処理され、前述の指紋画像データとして生成される。

#### 【0020】

次に、以上のように構成された指紋認証保管庫100及び指紋認証トークン200の動作を図4～図8のフローチャートに基づいて説明する。

(第1の実施の形態)

まず、図4及び図5のフローチャートに示す第1の実施の形態の動作から説明する。図4は、指紋認証保管庫100に対して物品を保管する場合の動作を示すフローチャートであり、利用者が自身の物品を保管する場合はステップS1のようにロックが外れている指紋認証保管庫100の扉101を開けて本体100Aの内部に物品を収納した後扉101を閉める。そして、指紋認証トークン200を差込口103に差込み（ステップS2）、さらに所定額のコインを投入口102に投入する（ステップS3）。

#### 【0021】

すると、処理装置111は、所定額のコインの投入を確認して錠制御装置113に扉101のロックを指示する（ステップS4）。これにより、扉101が本体100Aにロックされる（ステップS5）。その後、処理装置111はパスワードを発行して記憶装置112に記憶するとともに、そのパスワードを指紋認証トークン200の処理装置203に送る（ステップS6）。

#### 【0022】

指紋認証トークン200の処理装置203はパスワードを受信すると記憶装置204に記憶する（ステップS7）。このようにしてパスワードが指紋認証トークン200の記憶装置204に記憶された後、利用者はその指紋認証トークン200を指紋認証保管庫100の差込口103から引き抜き所持する（ステップS8）。

#### 【0023】

次に、指紋認証保管庫100の内部にこうして保管された物品を利用者が引き取る場合の動作を図5のフローチャートに基づいて説明する。

利用者が指紋認証保管庫100に保管中の物品の引き取りを行う場合は、当然その保管庫100の扉101は本体100Aにロックされている（ステップS11）。この場合、利用者は差込口103に自身が所持している指紋認証トークン200を差込み（ステップS12）、かつその指紋認証トークン200の指紋センサ202上に指をのせる（ステップS13）。

#### 【0024】

すると、指紋認証トークン200の処理装置203は、指紋センサ202によ

り検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップS14）。ここで、指紋認証トークン200の記憶装置204には、予め指紋センサ202により検出され処理装置203により処理された利用者自身の指紋画像データ中の特徴部分を示す照合情報が登録されており、処理装置203は、記憶装置204に保存されているこの登録情報とステップS14で抽出した照合情報とを比較する（ステップS15）。

## 【0025】

そして、双方の照合情報が不一致の場合はそのまま処理を終了するが、双方の照合情報が一致してステップS16の「照合情報が一致？」の判定がYESとなると、処理装置203は、予め記憶装置204に保存されているパスワードを指紋認証保管庫100の処理装置111に送信する（ステップS17）。この場合、処理装置111は指紋認証トークン200から送信されてきたパスワードと、記憶装置112に保存されているパスワードを比較する（ステップS18）。

## 【0026】

そして、双方のパスワードが不一致の場合はそのまま処理を終了するが、双方のパスワードが一致してステップS19の「パスワードが一致？」の判定がYESとなると、処理装置111は、錠制御装置113を制御して扉101の本体100Aへのロックを解除させる（ステップS20）。これにより、扉101を開くことができ、利用者は自身が本体100Aの内部に保管した物品を引き取ることができる。その後、利用者は自身の指紋認証トークン200を差込口103から引き抜く（ステップS21）。

## 【0027】

このように、利用者が物品を指紋認証保管庫100の内部に収納した後、所定額のコインを投入し、かつ指紋認証トークン200を差込口103に差し込むと、指紋認証保管庫100は扉101をロックするとともに、パスワードを発行し自身の記憶装置112に記憶し、かつ指紋認証トークン200に送出してその記憶装置204に記憶させる一方、保管した物品を引き取る場合に利用者がその指紋認証トークン200を保管庫100に差し込み、かつその指紋認証トークン2



00の指紋センサ202で検出された利用者の指紋画像とそのトークン200に予め登録されている指紋画像とが一致することにより、そのトークン200からパスワードが指紋認証保管庫100側へ送信されると、指紋認証保管庫100ではこのパスワードが自身に記憶されているものと一致した場合に扉101のロックを解除するようにしたものである。

## 【0028】

## (第2の実施の形態)

次に、図6は第2の実施の形態を示すフローチャートであり、指紋認証保管庫100に対して物品を保管する場合の動作を示すものである。

利用者が自身の物品を保管する場合はステップS31のように本体100Aに対しロックが解除されている扉101を開けて本体100Aの内部に物品を収納した後扉101を閉める。そして、指紋認証トークン200を差込口103に差込み(ステップS32)、かつ所定額のコインを投入口102に投入する(ステップS33)とともに、その指紋認証トークン200の指紋センサ202上に指をのせる(ステップS34)。

## 【0029】

すると、指紋認証トークン200の処理装置203は、指紋センサ202により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する(ステップS35)。そして、記憶装置204に保存されている登録情報とステップS35で抽出した照合情報とを比較する(ステップS36)。

## 【0030】

ここで、双方の照合情報が不一致の場合はそのまま処理を終了するが、双方の照合情報が一致してステップS37の「照合情報が一致？」の判定がYESとなると、処理装置203は、パスワードを発行して記憶装置204に記憶するとともに、そのパスワードを指紋認証保管庫100の処理装置111に送る(ステップS38)。この場合、処理装置111は、所定額のコインの投入を確認して錠制御装置113に扉101のロックを指示する(ステップS39)。これにより、扉101が本体100Aにロックされる(ステップS40)。その後、処理装

置 111 は指紋認証トークンから送られてきたパスワードを記憶装置 112 に保存する（ステップ S41）。このようにしてパスワードが指紋認証保管庫 100 の記憶装置 112 に保存された後、利用者はその指紋認証トークン 200 を指紋認証保管庫 100 の差込口 103 から引き抜き所持する（ステップ S42）。

#### 【0031】

このように、第 2 の実施の形態では、利用者が物品を保管するときには指紋認証トークン 200 における指紋認証の一致に応じて指紋認証トークン 200 がパスワードを発行して自身の記憶装置 204 に記憶するとともに、指紋認証保管庫 100 へ送信して記憶装置 112 に保存させ、かつ指紋認証保管庫 100 による扉 100 のロックを行わせるようにしたものである。なお、利用者が保管中の物品を引き取るときには図 5 のフローチャートに示す動作と同様の動作が行われる。即ち、指紋認証保管庫 100 と指紋認証トークン 200 間のパスワードの一致に基づき扉 101 のロックが解除される。

なお、第 1 及び第 2 の実施の形態では、指紋認証保管庫 100 の扉 101 のロックを解除するものとして、パスワードを用いているが、このパスワードはワンタイムパスワードでも良いし、指紋認証保管庫 100 や指紋認証トークン 200 に予め付与されている識別番号であっても良い。

#### 【0032】

##### （第 3 の実施の形態）

第 1 及び第 2 の実施の形態では、指紋認証保管庫 100 と指紋認証トークン 200 間のパスワードの一致に基づき扉 101 のロックを解除するものであるが、図 7 及び図 8 のフローチャートに示す第 3 の実施の形態では、指紋認証保管庫 100 と指紋認証トークン 200 間において利用者の指紋画像の一致に基づき扉 101 のロックを解除するものである。

#### 【0033】

まず、図 7 に示す、指紋認証保管庫 100 に物品を保管する場合の動作から説明する。利用者が自身の物品を保管する場合はステップ S51 のようにロックが解除されている指紋認証保管庫 100 の扉 101 を開けて本体 100A の内部に物品を収納した後扉 101 を閉める。そして、指紋認証トークン 200 を差込口

1 0 3 に差込み（ステップ S 5 2）、かつ所定額のコインを投入口 1 0 2 に投入する（ステップ S 5 3）とともに、その指紋認証トークン 2 0 0 の指紋センサ 2 0 2 上に指をのせる（ステップ S 5 4）。

#### 【 0 0 3 4 】

すると、指紋認証トークン 2 0 0 の処理装置 2 0 3 は、指紋センサ 2 0 2 により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップ S 5 5）。そして、抽出した照合情報を指紋認証保管庫 1 0 0 の処理装置 1 1 1 に送る（ステップ S 5 6）。この場合、処理装置 1 1 1 は、所定額のコインの投入を確認して錠制御装置 1 1 3 に扉 1 0 1 のロックを指示する（ステップ S 5 7）。これにより、扉 1 0 1 が本体 1 0 0 A にロックされる（ステップ S 5 8）。その後、処理装置 1 1 1 は指紋認証トークン 2 0 0 から送られてきた照合情報を記憶装置 1 1 2 に保存する（ステップ S 5 9）。このようにして照合情報が指紋認証保管庫 1 0 0 の記憶装置 1 1 2 に保存された後、利用者はその指紋認証トークン 2 0 0 を指紋認証保管庫 1 0 0 の差込口 1 0 3 から引き抜き所持する（ステップ S 6 0）。

#### 【 0 0 3 5 】

次に、指紋認証保管庫 1 0 0 の内部にこうして保管された物品を利用者が引き取る場合の動作を図 8 のフローチャートに基づいて説明する。

利用者が指紋認証保管庫 1 0 0 に保管中の物品の引き取りを行う場合は、その保管庫 1 0 0 の扉 1 0 1 はロックされている（ステップ S 6 1）。この場合、利用者は差込口 1 0 3 に自身が所持している指紋認証トークン 2 0 0 を差込み（ステップ S 6 2）、かつその指紋認証トークン 2 0 0 の指紋センサ 2 0 2 上に指をのせる（ステップ S 6 3）。

#### 【 0 0 3 6 】

すると、指紋認証トークン 2 0 0 の処理装置 2 0 3 は、指紋センサ 2 0 2 により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップ S 6 4）。そして、抽出した照合情報を指紋認証保管庫 1 0 0 の処理装置 1 1 1 に送出する（

ステップS65)。この場合、処理装置111は、扉101のロック時に記憶装置112に保存されている照合情報と、指紋認証トークン200からステップS65で送られてきた照合情報とを比較する（ステップS66）。

#### 【0037】

そして、双方の照合情報が不一致の場合はそのまま処理を終了するが、双方の照合情報が一致してステップS67の「照合情報が一致？」の判定がYESとなると、処理装置111は、錠制御装置113を制御して扉101のロックを解除させる（ステップS68）。これにより、扉101を開くことができ、利用者は自身が保管した物品を引き取ることができる。その後、利用者は自身の指紋認証トークン200を差込口103から引き抜く（ステップS69）。

#### 【0038】

このように、第3の実施の形態では、物品の保管時に扉101のロックを行うと同時に指紋認証トークン200から指紋認証保管庫100へ利用者の指紋画像を送信して記憶させる一方、保管中の物品の引き取り時には指紋認証保管庫100は指紋認証トークン200から送られてきた利用者の指紋画像と、記憶中の指紋画像とを比較し両者が一致すると扉101のロックを解除するようにしたものである。

#### 【0039】

##### （第4の実施の形態）

図14は指紋認証保管庫の第4の実施の形態を示す図である。前述の例では、物品を保管する場合、保管庫100内に1つの保管部を設けた例を示したが、第4の実施の形態では、図14に示すように指紋認証保管庫100にそれぞれ独立して物品の保管が可能な複数（9個）の保管部を設けこれらの各保管部に対応してそれぞれ複数の扉101-1～101-9を付けるようにしたものである。この他、この指紋認証保管庫100には各扉101-1～101-9の何れかを指定するためのテンキー141と、各種の表示を行う表示部142が設けられている。

#### 【0040】

図15は、図14に示す指紋認証保管庫100の構成を示すブロック図であり

、前述した処理装置 1 1 1 と、記憶装置 1 1 2 と、錠制御装置 1 1 3 とが設けられているとともに、錠制御装置 1 1 3 は、複数の扉 1 0 1 - 1 ~ 1 0 1 - 9 に接続され各扉 1 0 1 - 1 ~ 1 0 1 - 9 のロック及びロック解除を行う。また、処理装置 1 1 1 は、コイン投入口 1 0 2 に投入されたコインを検出して所定の処理を行うとともに、差込口 1 0 3 に指紋認証トークン 2 0 0 が差し込まれるとその指紋認証トークン 2 0 0 からの指紋情報の認証処理等を行う他に、テンキー 1 4 1 の操作入力や表示部 1 4 2 の表示制御等を行う。

#### 【 0 0 4 1 】

次に、以上のように構成された指紋認証保管庫 1 0 0 の要部動作を図 1 6 及び図 1 7 のフローチャートに基づいて説明する。まず、図 1 6 のフローチャートに基づき扉 1 0 1 のロック動作から説明する。

利用者が自身の物品を保管する場合はステップ S 7 1 のようにロックが外れている指紋認証保管庫 1 0 0 の扉 1 0 1 - i を開けて対応の保管部に物品を収納した後扉 1 0 1 - i を閉める（ステップ S 7 2）。すると、処理装置 1 1 1 はこれを検出して表示部 1 4 2 の表示画面に、閉じた扉 1 0 1 - i の番号を表示する。利用者はこの表示を確認して、扉をロックする場合は該当扉 1 0 1 - i の番号に対応するテンキー 1 4 1 の数字キーを押下する（ステップ S 7 3）。

#### 【 0 0 4 2 】

すると、ステップ S 7 4 の「扉 1 0 1 - i をロックするか？」の判定が「Y」となり、ステップ S 7 5 へ移行する。ステップ S 7 5 では、利用者により指紋認証トークン 2 0 0 が差込口 1 0 3 に差込まれ、さらにステップ S 7 6 で所定額のコインが投入口 1 0 2 に投入される。

#### 【 0 0 4 3 】

この場合、処理装置 1 1 1 は、所定額のコインの投入を確認して錠制御装置 1 1 3 に扉 1 0 1 - i のロックを指示する（ステップ S 7 7）。これにより、扉 1 0 1 - i が本体 1 0 0 A にロックされる（ステップ S 7 8）。その後、処理装置 1 1 1 はパスワードを発行して、パスワード及びロックした扉 1 0 1 - i の番号を記憶装置 1 1 2 に記憶するとともに、そのパスワード及びロックされた扉 1 0 1 - i の番号を指紋認証トークン 2 0 0 の処理装置 2 0 3 に送る（ステップ S 7

9)。

【 0 0 4 4 】

指紋認証トークン 2 0 0 の処理装置 2 0 3 はパスワード及びロックした扉 1 0 1 - i の番号を受信すると記憶装置 2 0 4 に記憶する (ステップ S 8 0) 。このようにしてパスワード及びロックした扉 1 0 1 - i の番号が指紋認証トークン 2 0 0 の記憶装置 2 0 4 に記憶された後、利用者はその指紋認証トークン 2 0 0 を指紋認証保管庫 1 0 0 の差込口 1 0 3 から引き抜いて所持する (ステップ S 8 1) 。

【 0 0 4 5 】

次に、図 1 7 のフローチャートに基づき扉 1 0 1 のロック解除動作について説明する。

利用者が指紋認証保管庫 1 0 0 の保管部から自身の保管物品の引き取りを行う場合は、当然その保管部の扉 1 0 1 - i はロックされている (ステップ S 9 1) 。この場合、利用者は差込口 1 0 3 に自身が所持している指紋認証トークン 2 0 0 を差込む (ステップ S 9 2) 。すると、指紋認証トークン 2 0 0 の記憶装置 2 0 4 に記憶されている扉 1 0 1 - i の番号が読み出されて表示部 1 4 2 に表示される。なお、記憶部 2 0 4 に複数の扉の番号が記憶されている場合は、これらの全ての番号がロックされている扉の番号として表示部 1 4 2 に表示される。この場合、利用者はロックを解除したい扉の番号をテンキー 1 4 1 の該当数字キーで選択操作する (ステップ S 9 3) 。そして、その後指紋認証トークン 2 0 0 の指紋センサ 2 0 2 上に指をのせる (ステップ S 9 4) 。

【 0 0 4 6 】

すると、指紋認証トークン 2 0 0 の処理装置 2 0 3 は、指紋センサ 2 0 2 により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する (ステップ S 9 5) 。そして、処理装置 2 0 3 は、記憶装置 2 0 4 に保存されている登録情報とステップ S 9 5 で抽出した照合情報とを比較する (ステップ S 9 6) 。そして、双方の照合情報が不一致の場合はそのまま処理を終了するが、双方の照合情報が一致してステップ S 9 7 の「照合情報が一致？」の判定が Y E S となると、処理装置 2 0

3 は、予め記憶装置 2 0 4 に保存されているパスワード及びロックした扉 1 0 1 - i の番号を指紋認証保管庫 1 0 0 の処理装置 1 1 1 に送信する（ステップ S 9 8）。この場合、処理装置 1 1 1 は指紋認証トークン 2 0 0 から送信されてきたパスワードと、記憶装置 1 1 2 に保存されているパスワードを比較する（ステップ S 9 9）。

【 0 0 4 7 】

そして、双方のパスワードが不一致の場合はそのまま処理を終了するが、双方のパスワードが一致してステップ S 1 0 0 の「パスワードが一致？」の判定が Y E S となると、処理装置 1 1 1 は、錠制御装置 1 1 3 を制御して扉 1 0 1 - i の本体 1 0 0 A へのロックを解除させる（ステップ S 1 0 1）。これにより、扉 1 0 1 - i を開くことができ、利用者は自身が保管部に保管した物品を引き取ることができる。なお、この場合、処理装置 1 1 1 は記憶装置 1 1 2 に保存されている扉 1 0 1 - i の番号を消去する。その後、利用者は自身の指紋認証トークン 2 0 0 を差込口 1 0 3 から引き抜く（ステップ S 1 0 2）。

【 0 0 4 8 】

このように、利用者が物品を指紋認証保管庫 1 0 0 の内部に収納した後、所定額のコインを投入し、かつ指紋認証トークン 2 0 0 を差込口 1 0 3 に差し込むと、指紋認証保管庫 1 0 0 は扉 1 0 1 をロックするとともに、パスワードを発行し自身の記憶装置 1 1 2 に記憶し、かつ指紋認証トークン 2 0 0 に送出してその記憶装置 2 0 4 に記憶させる一方、保管した物品を引き取る場合に利用者がその指紋認証トークン 2 0 0 を保管庫 1 0 0 に差し込み、かつその指紋認証トークン 2 0 0 の指紋センサ 2 0 2 で検出された利用者の指紋画像とそのトークン 2 0 0 に予め登録されている指紋画像とが一致することにより、そのトークン 2 0 0 からパスワードが指紋認証保管庫 1 0 0 側へ送信されると、指紋認証保管庫 1 0 0 ではこのパスワードが自身に記憶されているものと一致した場合に扉 1 0 1 のロックを解除するようにしたものである。

【 0 0 4 9 】

このように、本発明では、指紋認証トークンを用いた利用者本人の認証に基づき、物品保管庫の扉のロック及びロック解除を行うようにしたものである。この

ような指紋認証保管庫をコインロッカー等の物品保管庫に適用すれば、従来、こうした物品保管庫に付与されていた鍵の使用に基づく解錠や施錠を排除することができ、したがって紛失鍵の使用に基づく物品保管庫の不正な解錠を阻止することができる。また、第三者が指紋認証トークンを利用して物品保管庫を解錠しようとしても、第三者の指紋画像は本来の利用者の指紋画像が異なり、物品保管庫の扉のロックを解除できないことから、同様に第三者による物品保管庫の解錠を阻止できる。

なお、図4～図8に示す各ステップの実行順序は一例を示したものであって、全体の動作に矛盾を来さない場合は各ステップの実行順序を変更しても良い。

#### 【0050】

また、本実施の形態では、指紋認証トークン200内の指紋センサ201、処理装置203、記憶装置204をワンチップで構成した第1の構成例について説明したが、上記第1の構成例の他に、指紋センサ202をワンチップ化し、このワンチップ指紋センサ202に、バスを介して処理装置203を接続し、さらに処理装置203にバスを介して記憶装置204を接続する第2の構成例がある。さらに、指紋センサ202と処理装置203をワンチップ化し、このワンチップ化された処理装置203にバスを介して記憶装置204を接続する第3の構成例がある。

#### 【0051】

また、指紋認証トークン200と指紋認証保管庫200間で送受される信号を送信側で暗号化し、受信側でその暗号化データを復号化することにより、システムのセキュリティを向上させることができる。

また、本実施の形態では、指紋の認証に基づいて物品保管庫の解錠を行うようにしたが、指の大きさ、手形、静脈パターン、人相、虹彩及び声紋などの利用者固有の生体情報や、利用者のサイン（筆跡）等により利用者本人であることを認証して解錠するようにしても良い。

#### 【0052】

図11は、前述の指紋認証トークン200を含む認証トークン300と、認証トークン300の認証を利用してユーザ（利用者）にサービスを提供する前述の



指紋認証保管庫 1 0 0 を含む利用機器 4 0 0 とからなる一般的な認証システムの構成を示すブロック図である。

この認証システムでは、ユーザ固有の生体情報として指紋を用いる場合を例として説明する。

#### 【 0 0 5 3 】

認証トークン 3 0 0 には、指紋（生体情報）を読み取るセンサ 3 1 1、ユーザ本人の登録指紋データ 3 1 2 A やユーザ情報 3 1 2 B を記憶する記憶回路 3 1 2、センサ 3 1 1 での読み取り結果を示すセンシングデータ 3 1 1 A を、記憶回路 3 1 2 に記憶されている登録指紋データ 3 1 2 A を用いて照合する照合回路 3 1 3、この照合回路 3 1 3 での照合結果を含む認証データ 3 1 3 A を通信データ 3 0 1 A として認証トークン 3 0 0 の外部へ送信する通信回路 3 1 4 が設けられており、これら回路部を一体として形成する認証トークン 3 0 0 が利用機器 4 0 0 に対して着脱自在に接続される。

利用機器 4 0 0 には、認証トークン 3 0 0 からの通信データ 3 0 1 A を受信する通信回路 4 2 1 と、受信した通信データ 3 0 1 A に含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置 4 2 2 とが設けられている。

#### 【 0 0 5 4 】

次に、図 1 1 に示す認証システムの動作について説明する。

ユーザは事前に、自分の所持する認証トークン 3 0 0 の記憶回路 3 1 2 に、自分の登録指紋データ 3 1 2 A やサービスを利用するためのパスワードや個人情報などからなるユーザ情報 3 1 2 B を記憶させておく。

利用機器 4 0 0 を利用する際、まずユーザは自分の認証トークン 4 0 0 を利用機器 4 0 0 へ接続し、指をそのセンサ 3 1 1 へ置く。これにより認証トークン 3 0 0 のセンサ 3 1 1 でユーザの指紋が読み取られセンシングデータ 3 1 1 A として出力される。このセンシングデータ 3 1 1 A は照合回路 3 1 3 において記憶回路 3 1 2 の登録指紋データ 3 1 2 A を用いて照合される。そして、その照合結果を含む認証データ 3 1 3 A が出力される。このとき照合回路 3 1 3 は、記憶回路 3 1 2 に予め記憶回路 1 2 に格納されているユーザ ID、パスワード、個人情報

などのユーザ情報 3 1 2 B を読み出し、認証データ 3 1 3 A へ含めて出力する。

【 0 0 5 5 】

通信回路 3 1 4 では、照合回路 3 1 3 からの認証データ 3 1 3 A を通信データ 3 0 1 A として利用機器 4 0 0 へ送信する。

利用機器 4 0 0 の通信回路 4 2 1 では、認証トークン 3 0 0 の通信回路 3 1 4 から送信された通信データ 3 0 1 A を受信し、認証データ 3 1 3 A と同じ内容の認証データ 4 2 1 A として出力する。処理装置 4 2 2 では、この認証データ 4 2 1 A を受け取ってその認証データ 4 2 1 A に含まれる照合結果を参照する。そして、その照合結果が一致を示す場合、処理装置 4 2 2 においてユーザの所望する所定の処理が実行される。

【 0 0 5 6 】

このように、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ 3 1 1 と、ユーザの指紋を照合するための登録指紋データ 3 1 2 A が予め格納されている記憶回路 3 1 2 と、この記憶回路 3 1 2 に記憶されている登録指紋データ 3 1 2 A を用いてセンサ 3 1 1 からのセンシングデータ 3 1 1 A を照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路 3 1 3 と、この照合回路 3 1 3 からの認証データを通信データ 3 0 1 A として利用機器 4 0 0 へ送信する通信回路 3 1 4 とを、認証トークン 3 0 0 として一体として形成したものである。

【 0 0 5 7 】

そして、認証に応じて所定の処理を行う利用機器 4 0 0 をユーザが利用する場合には、認証トークン 3 0 0 をその利用機器 4 0 0 へ接続し、その認証トークン 3 0 0 でユーザの生体情報に基づきユーザ認証を行い、利用機器 4 0 0 へ通知するようにしたものである。

また、利用機器 4 0 0 に、認証トークン 3 0 0 から送信された通信データ 3 0 1 A を受信し認証データ 4 2 1 A として出力する通信回路 4 2 1 と、この通信回路 4 2 1 からの認証データ 4 2 1 A に含まれる照合結果に基づき所定の処理を行う処理装置 4 2 2 とを設け、この利用機器 4 0 0 とは独立した各ユーザが個々の持つ認証トークン 3 0 0 での認証結果に基づき所定の処理を行うようにしたもの

である。

【 0 0 5 8 】

したがって、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。なお、認証トークン 3 0 0 については、センサ、記憶回路および照合回路などを 1 チップの半導体装置として形成する技術（例えば、特開 2 0 0 0 - 2 4 2 7 7 1 号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

【 0 0 5 9 】

さらに、記憶回路 3 1 2 にユーザ I D やパスワードさらには個人情報などのユーザ情報 3 1 2 B を予め記憶しておき、これらを認証データ 3 1 3 A に含めて利用機器 4 0 0 へ送信するようにしたので、利用機器 4 0 0 の処理装置 4 2 2 において、その認証データに含まれるユーザ情報 3 1 2 B、例えばユーザ I D やパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報 3 1 2 B の個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

【 0 0 6 0 】

なお、利用機器 4 0 0 に図示しない乱数発生回路及び復号回路を設け、かつ認証トークン 3 0 0 に図示しない暗号化回路を設けて、利用機器 4 0 0 と認証トークン 3 0 0 間で通信されるデータの暗号化することにより、セキュリティの向上を図ることができる。

## 【 0 0 6 1 】

即ち、利用機器 4 0 0 は、認証トークン 3 0 0 側からのアクセス時に乱数発生回路により乱数を発生させてこの乱数を通信回路 4 2 1 から認証トークン 3 0 0 へ送信して暗号化回路に記憶させる一方、認証トークン 3 0 0 の暗号化回路は照合回路 3 1 3 から出力された認証データ 3 1 3 A と、記憶した乱数との和を演算してその演算結果を、予め記憶回路 3 1 2 に記憶してある共通鍵により暗号化して暗号化データとして利用機器 4 0 0 側へ送信する。利用機器 4 0 0 では、通信回路 4 2 1 により受信したこの暗号化データを復号回路が共通鍵を用いて復号化するとともに復号化したデータから乱数発生回路が発生した前記乱数を減算することにより認証データ 4 2 1 A として処理回路 4 2 2 へ出力する。なお、上記の例では、認証トークン 3 0 0 及び利用機器 4 0 0 の双方に共通鍵を持たせて、それぞれ暗号化及び復号化を行わせているが、認証トークン 3 0 0 に秘密鍵を、利用機器 4 0 0 に公開鍵を持たせてそれぞれ暗号化処理及び復号化処理を行わせることもできる。

## 【 0 0 6 2 】

次に、図 1 2 を参照して、本認証システムの第 2 の構成例について説明する。図 1 2 は、図 1 1 に示す第 1 の構成例のうち、認証トークン 3 0 0 の出力段にデータ変換モジュール 3 3 0 を付加したものである。

このデータ変換モジュール 3 3 0 には、認証トークン 3 0 0 の通信回路 3 1 4 から出力された通信データを、利用機器 4 0 0 で受信・解読可能なデータ形式へ変換するプロトコル変換回路 3 3 1 が設けられている。

## 【 0 0 6 3 】

このように、認証トークン 3 0 0 に着脱自在に取り付けられるデータ変換モジュール 3 3 0 を介して、所望の利用機器 4 0 0 と認証トークン 3 0 0 とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが 1 つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。

以上では、データ変換モジュール 3 3 0 を認証トークン 3 0 0 に対して着脱自在に取り付ける場合を例として説明したが、認証トークン 3 0 0 内部にプロトコル変換回路 3 3 1 を設けてもよく、さらにコンパクトに構成できる。

#### 【 0 0 6 4 】

次に、図 1 3 を参照して、本認証システムの第 3 の構成例について説明する。図 1 3 は、図 1 1 に示す第 1 の構成例のうち、認証トークン 3 0 0 の出力段に無線モジュール 3 4 0 を付加したものである。

この無線モジュール 3 4 0 には、認証トークン 3 0 0 の通信回路 3 1 4 から出力された通信データを、利用機器 4 0 0 で受信・解読可能なデータ形式へ変換するプロトコル変換装置 3 4 1 と、このプロトコル変換装置 3 4 1 からの通信データを無線区間を介して利用機器 4 0 0 へ送信する無線回路 3 4 2 とが設けられている。この場合、利用機器 4 0 0 側にも無線回路 4 2 3 を設ける必要がある。

#### 【 0 0 6 5 】

このように、認証トークン 3 0 0 に着脱自在に取り付けられる無線モジュール 3 4 0 を用いて、所望の利用機器 4 0 0 と認証トークン 3 0 0 とを接続するようになったので、ユーザは、認証トークン 3 0 0 を利用機器 4 0 0 に直接接続することなく、例えば自分の手元で認証トークン 3 0 0 を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器 4 0 0 に対して認証トークン 3 0 0 を接続する作業や、利用機器 4 0 0 に接続されている状態の認証トークン 3 0 0 を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

#### 【 0 0 6 6 】

なお、利用機器 4 0 0 と認証トークン 3 0 0 の通信プロトコルが同一の場合は、無線モジュール 3 4 0 のプロトコル変換回路 3 4 1 を省略することも可能である。また、無線回路 3 4 2 の代わりに、赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール 3 4 0 を認証トークン 3 0 0 に対して着脱自在に取り付ける場合を例として説明したが、認証トークン 3 0 0 内部に無線回路 3 4 2 やプロトコル変換回路 3 4 1 を設けてもよく、さらにコンパクトに構成できる。

【 0 0 6 7 】

【発明の効果】

以上説明したように本発明によれば、本体内部への物品の保管時及び本体内部に保管された物品の取り出し時にはそれぞれ本体の扉のロック及びロック解除が行われるとともに、利用者の生体情報の認証に基づいて扉のロックを解除可能な生体情報認証保管庫を設け、かつこの生体情報認証保管庫に、扉のロック及びロック解除を行う駆動手段と、利用者の生体情報を記憶する記憶手段と、処理手段とを設け、処理手段は利用者の生体情報を検出するセンサの検出情報と記憶手段の記憶情報との一致に基づき駆動手段を制御し扉のロックを解除するようにしたので、このような生体情報認証保管庫をコインロッカー等の物品保管庫に適用すれば、従来、こうした物品保管庫に付与されていた鍵の使用に基づく解錠や施錠を排除することができ、したがって第三者の紛失鍵の使用に基づく物品保管庫の不正な解錠を阻止することができる。また、第三者が前記センサを用いて物品保管庫を解錠しようとしても、第三者の生体情報は記憶手段に記憶されている本来の利用者の生体情報と異なり、物品保管庫の扉のロックを解除できないことから、同様に第三者による物品保管庫の解錠を阻止できる。

【 0 0 6 8 】

また、記憶手段に利用者の指紋画像を記憶するとともに、利用者の指紋画像を検出する指紋センサを前記センサとして設け、処理手段は本体内部への物品の保管時に、この指紋センサを内蔵した指紋認証トークンからの指紋画像を受信すると扉をロックしかつ受信した指紋画像を記憶手段に記憶する一方、本体内部に保管された物品の取り出し時に指紋認証トークンから送信された利用者の指紋画像を受信するとこの受信指紋画像が記憶手段の記憶情報と一致する場合は扉のロックを解除させるようにしたので、同様に第三者による物品保管庫の解錠が阻止され、セキュリティが向上する。

また、処理手段は、本体内部への物品の保管時に指紋認証トークンが本体に差し込まれると扉をロックするとともに、パスワードを発生してこのパスワードを記憶手段に記憶し、かつ指紋認証トークンへ送信して記憶させる一方、本体内部に保管された物品の取り出し時に指紋認証トークンから出力される前記センサに

よる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は扉のロックを解除するようにしたので、物品を保管した利用者以外の第三者による保管庫の解錠が阻止され、同様にセキュリティが向上する。

【 0 0 6 9 】

また、処理手段は、本体内部への物品の保管時に指紋認証トークンから出力されるセンサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると扉をロックし、かつ受信したパスワードを記憶手段に記憶するとともに、本体内部に保管された物品の取り出し時に指紋認証トークンから出力されるセンサによる検出指紋画像と登録指紋画像との一致に基づくパスワードを受信すると、この受信パスワードと記憶手段のパスワードとが一致する場合は扉のロックを解除するようにしたので、同様に物品を保管した利用者以外の第三者による保管庫の解錠が阻止され、セキュリティが向上する。

【図面の簡単な説明】

【図 1】 本発明を適用した指紋認証保管庫の外観を示す図である。

【図 2】 前記指紋認証保管庫の扉のロック及びロック解除を行う指紋認証トークンの外観を示す図（図 2（a））及びその構成を示すブロック図（図 2（b））である。

【図 3】 前記指紋認証保管庫の構成を示すブロック図である。

【図 4】 物品を保管する際の前記指紋認証保管庫及び指紋認証トークンの動作を示すフローチャートである。

【図 5】 保管した物品を取り出す際の前記指紋認証保管庫及び指紋認証トークンの動作を示すフローチャートである。

【図 6】 物品を保管する際の前記指紋認証保管庫及び指紋認証トークンの動作を示すフローチャートである。

【図 7】 物品を保管する際の前記指紋認証保管庫及び指紋認証トークンの動作を示すフローチャートである。

【図 8】 保管した物品を取り出す際の前記指紋認証保管庫及び指紋認証トークンの動作を示すフローチャートである。

【図 9】 前記指紋認証トークンを構成する指紋センサの詳細構成を示す図である。

【図 1 0】 前記指紋センサ内の容量検出回路の回路図である。

【図 1 1】 認証トークンおよび利用機器からなる認証システムの第 1 の構成例を示すブロック図である。

【図 1 2】 認証トークンおよび利用機器からなる認証システムの第 2 の構成例を示すブロック図である。

【図 1 3】 認証トークンおよび利用機器からなる認証システムの第 3 の構成例を示すブロック図である。

【図 1 4】 指紋認証保管庫の他の構成例を示す図である。

【図 1 5】 図 1 4 に示す指紋認証保管庫の構成を示すブロック図である。

【図 1 6】 図 1 5 に示す指紋認証保管庫及び前記指紋認証トークンの要部動作を示すフローチャートである。

【図 1 7】 図 1 5 に示す指紋認証保管庫及び前記指紋認証トークンの要部動作を示すフローチャートである。

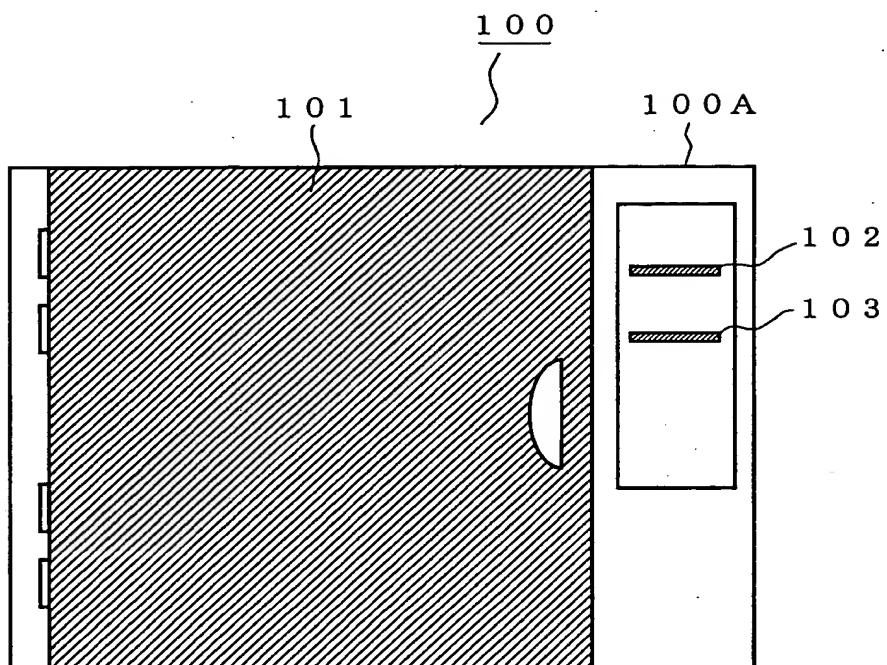
【符号の説明】

1 0 0 …指紋認証保管庫、1 0 0 A …本体、1 0 1, 1 0 1 - 1 ~ 1 0 1 - 9 …扉、1 0 2 …コイン投入口、1 0 3 …差込口、1 1 1, 2 0 3 …処理装置、1 1 2, 2 0 4 …記憶装置、1 4 1 …テンキー、1 4 2 …表示部、2 0 0 …指紋認証トークン、2 0 2 …指紋センサ、2 1 1 …半導体基板、2 1 2 …下層絶縁膜、2 1 3 …配線、2 1 4 …層間絶縁膜、2 1 5 …センサ電極、2 1 7 …パシベーション膜、2 1 8 …容量検出回路。

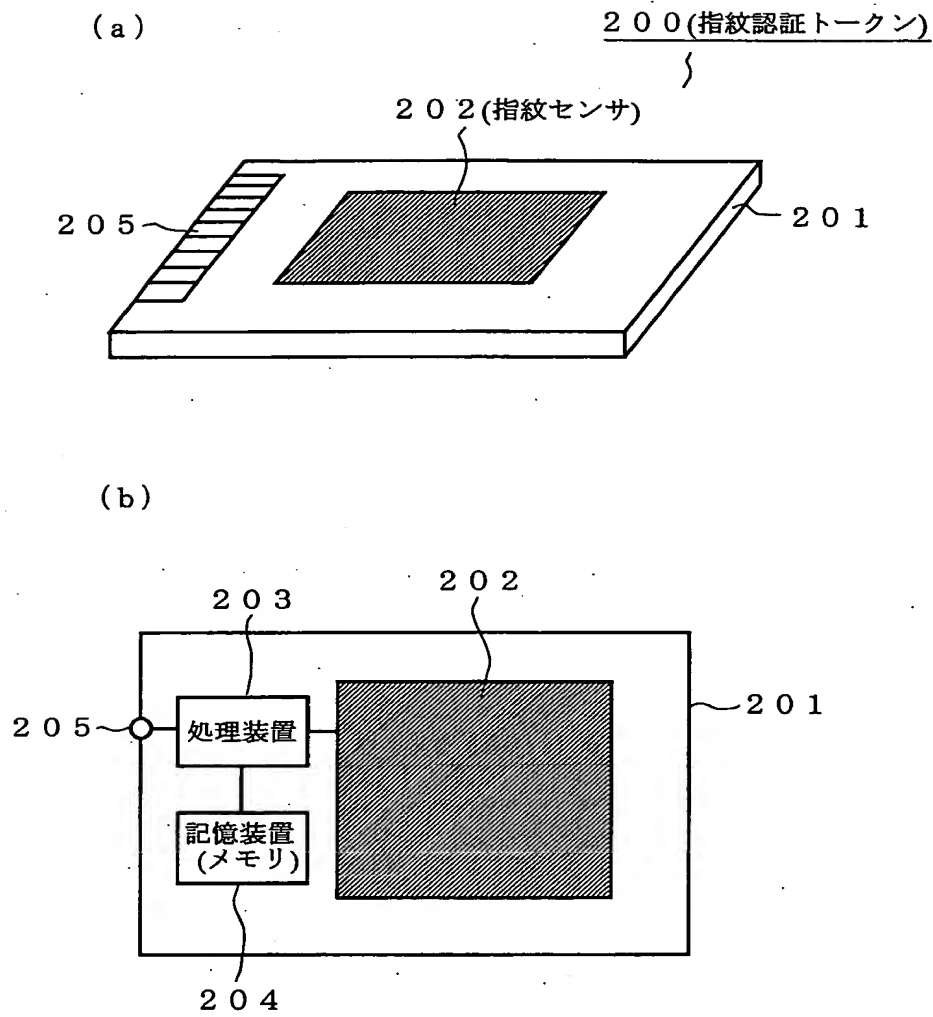


【書類名】 図面

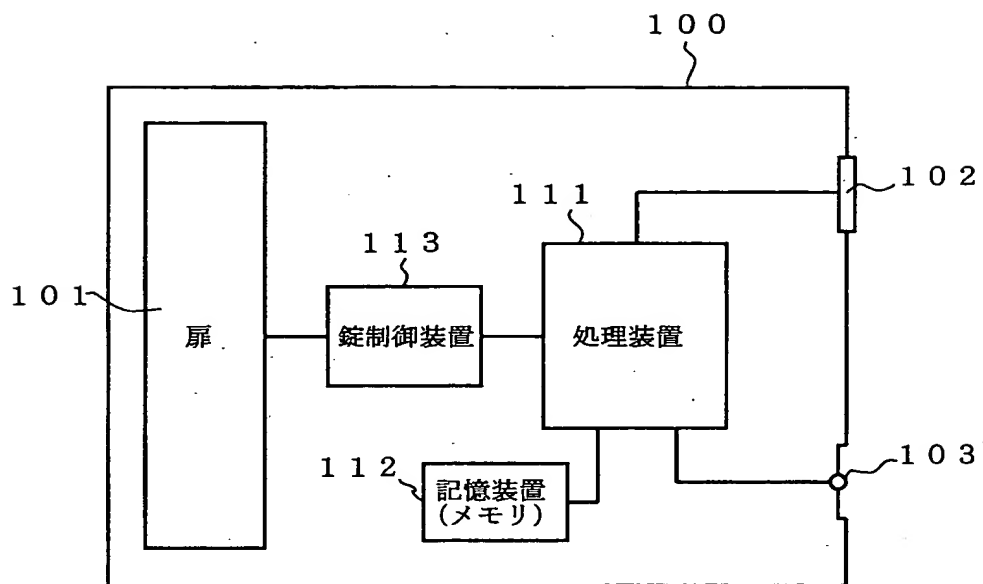
【図 1】



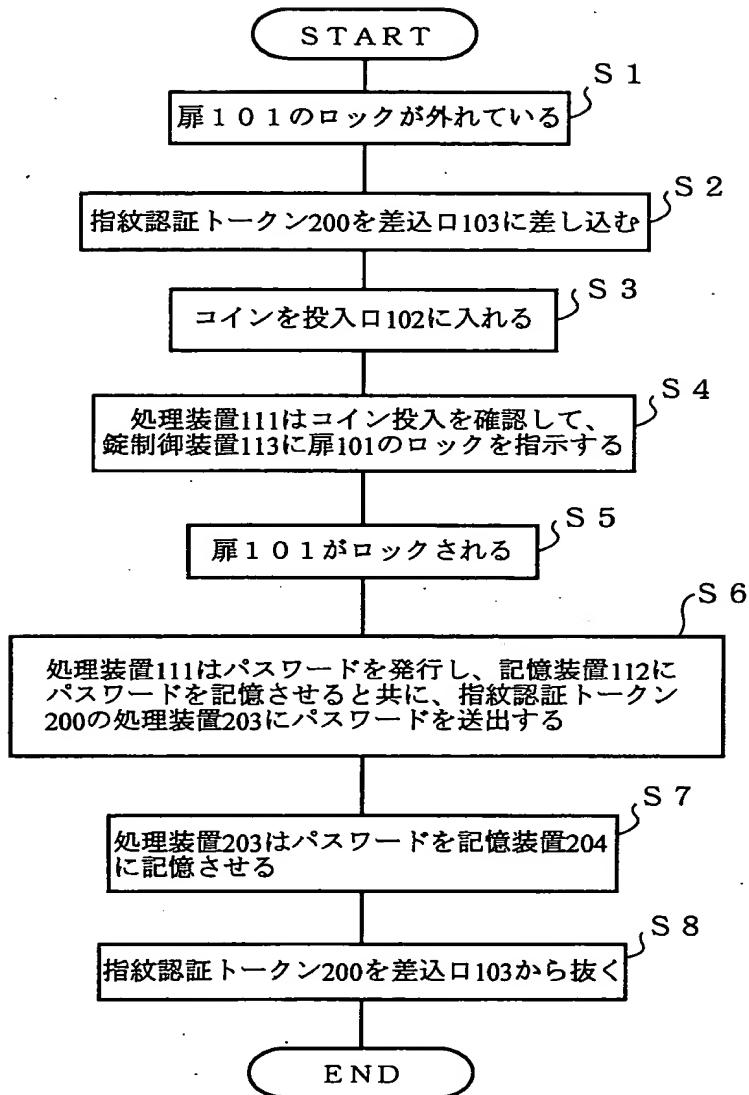
【図 2】



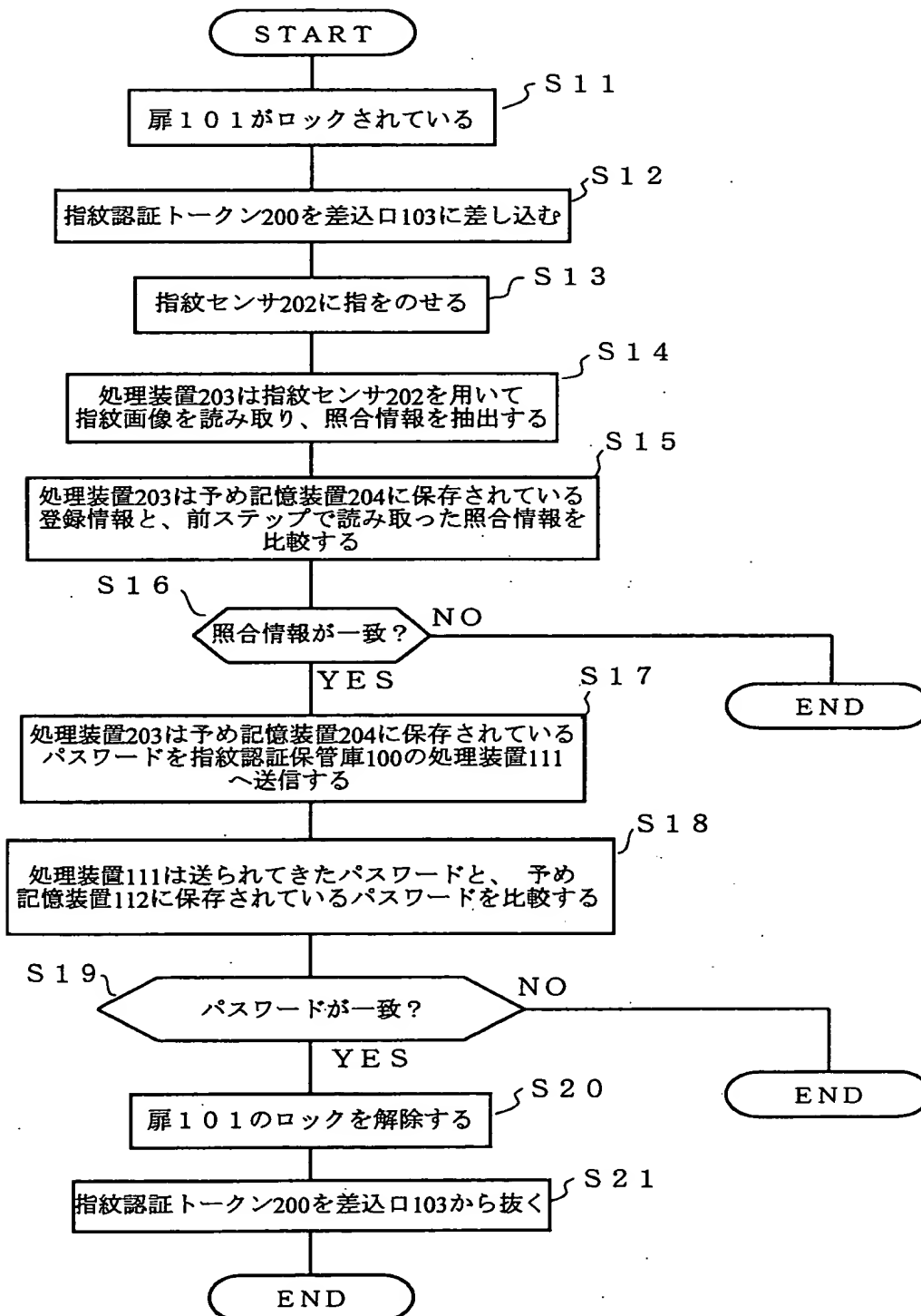
【図 3】



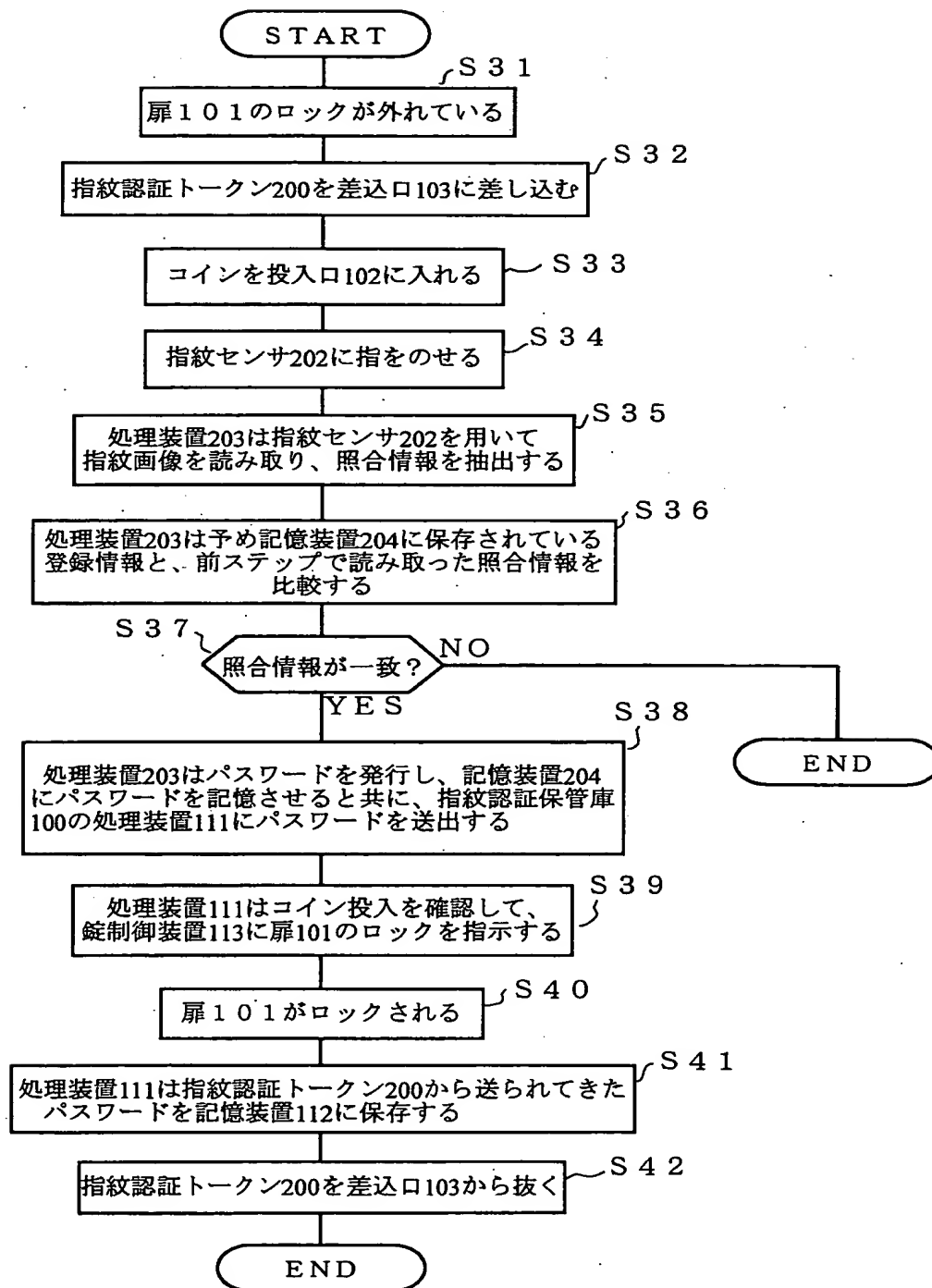
【図 4】



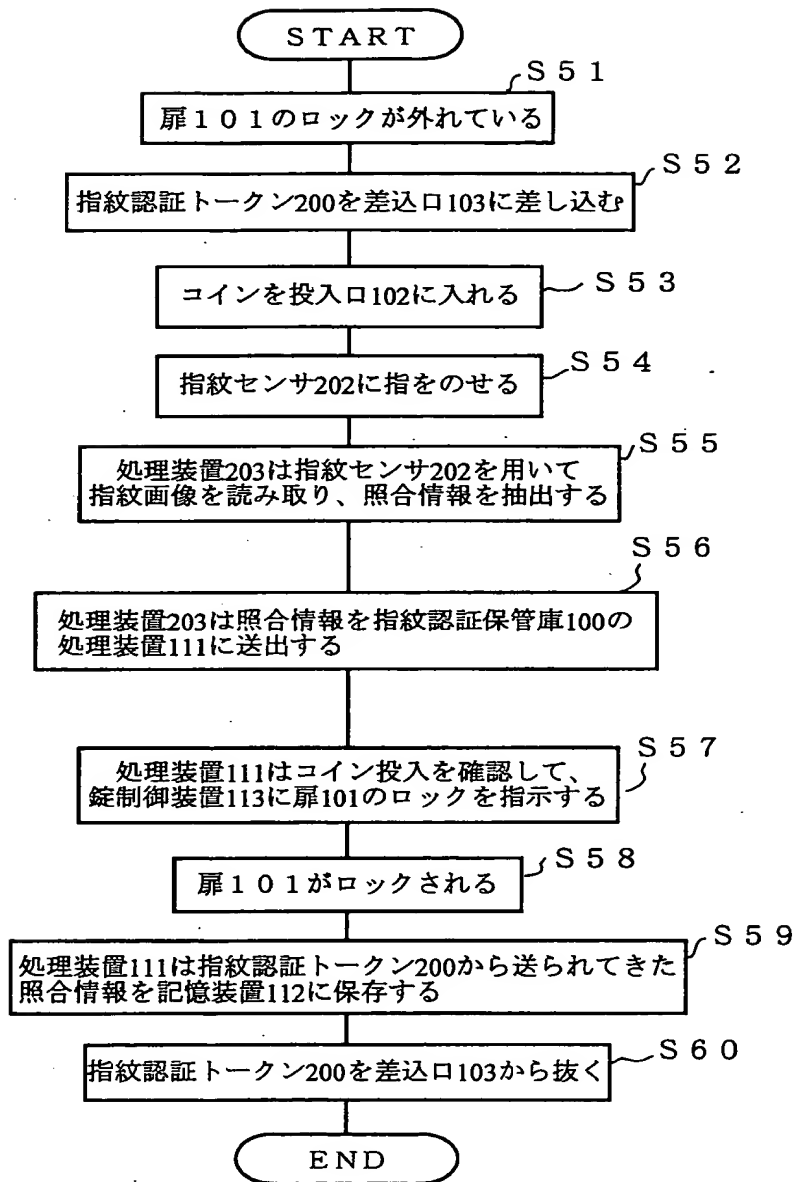
【図 5】



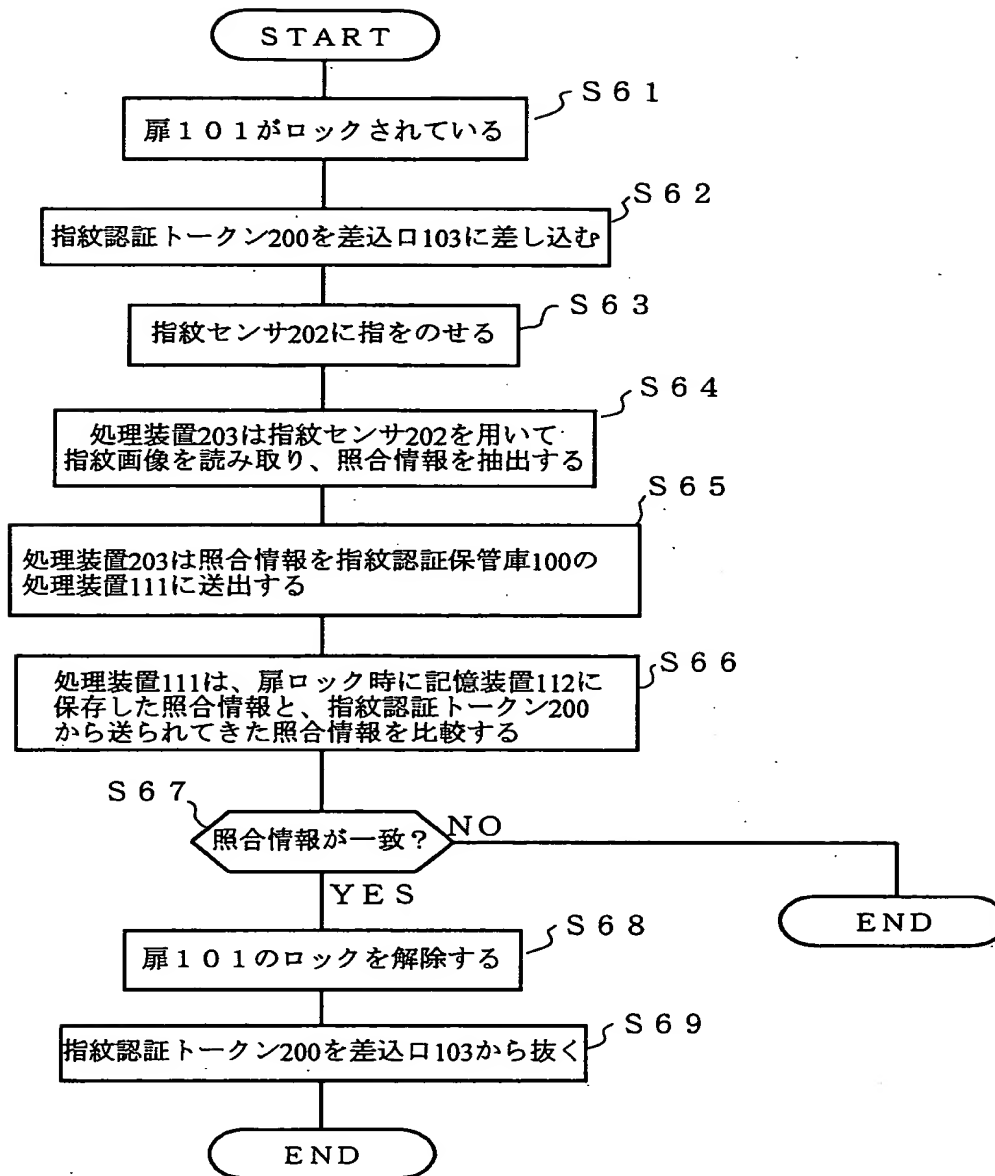
【図 6】



【図 7】

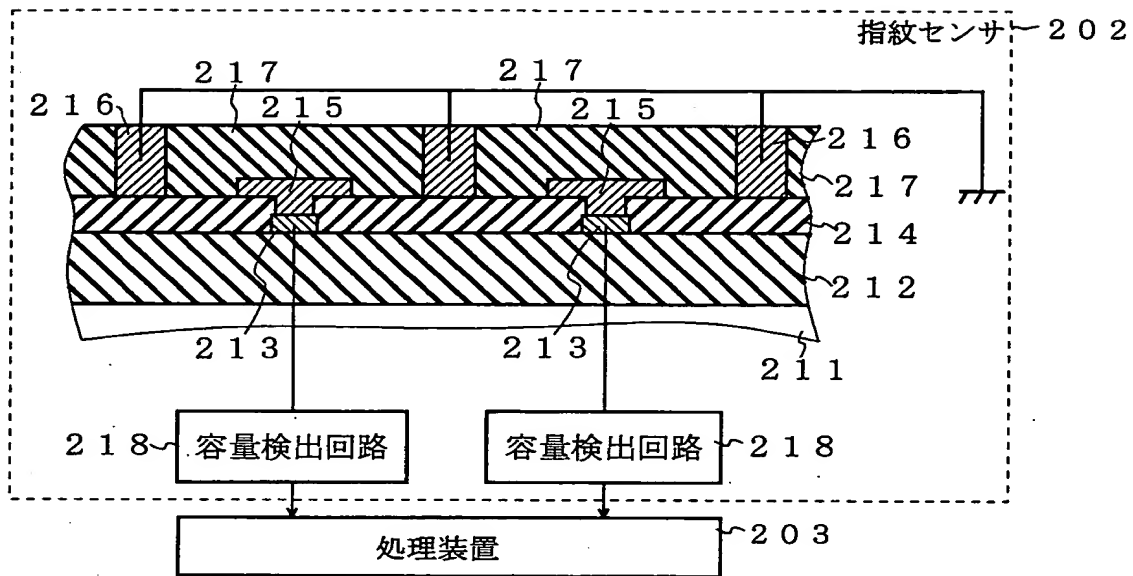


【図 8】

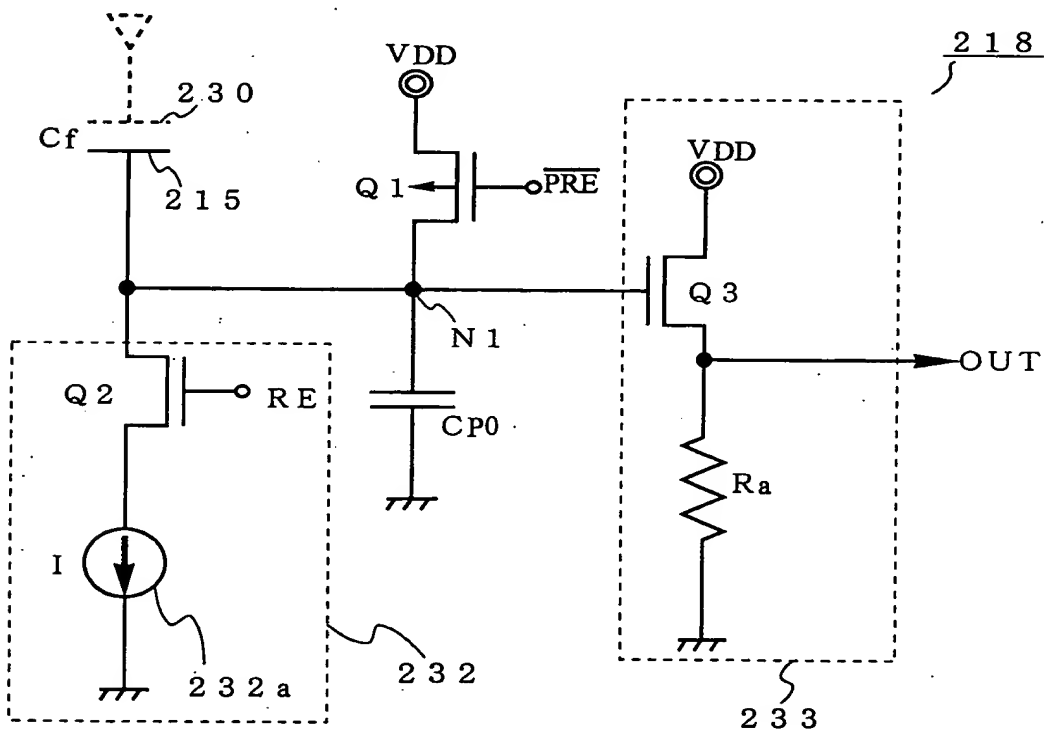




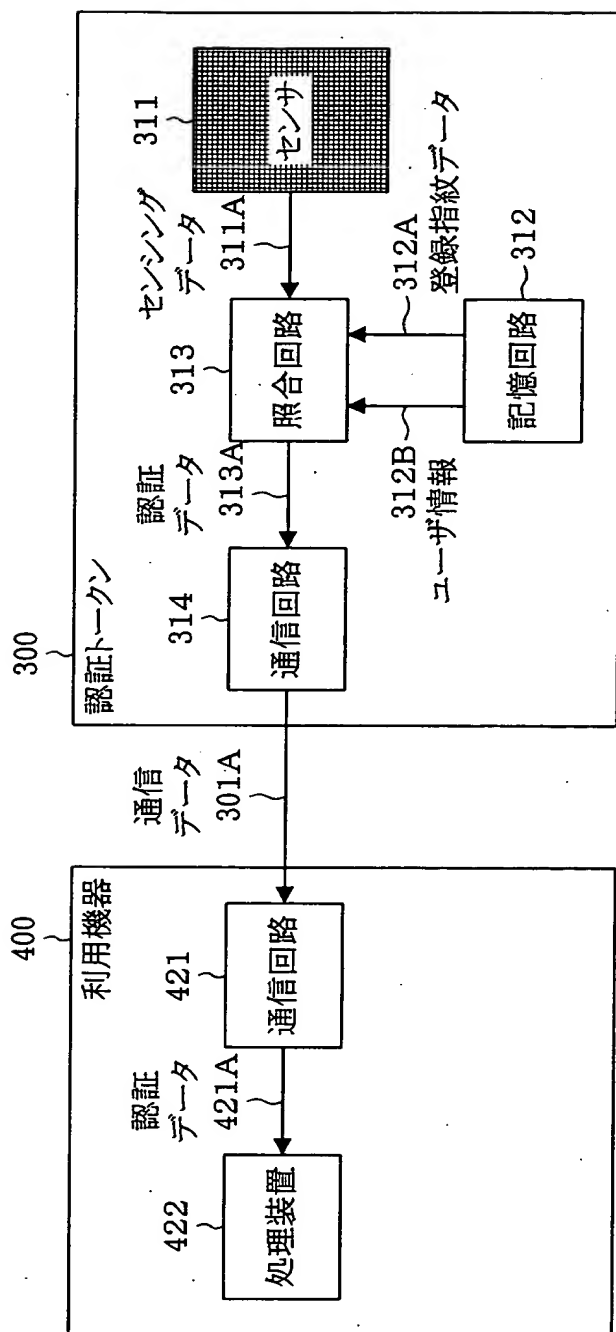
【図9】



【図10】



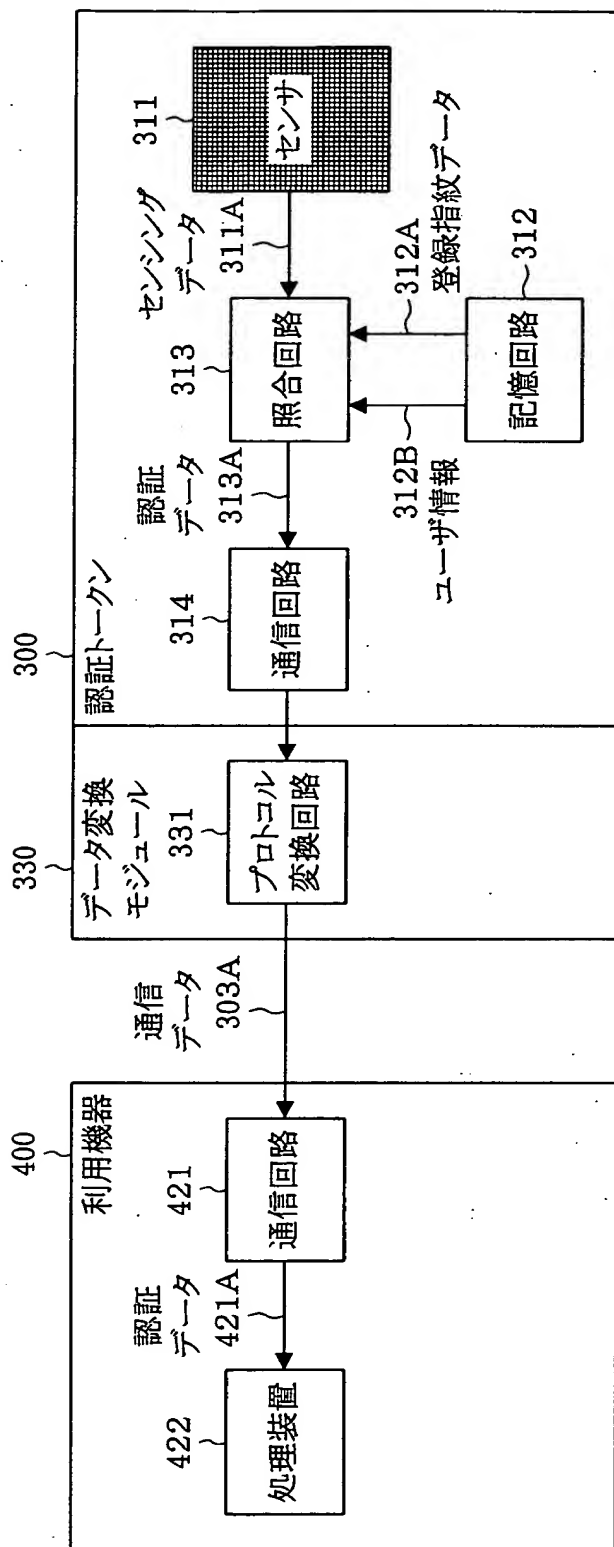
【図 11】



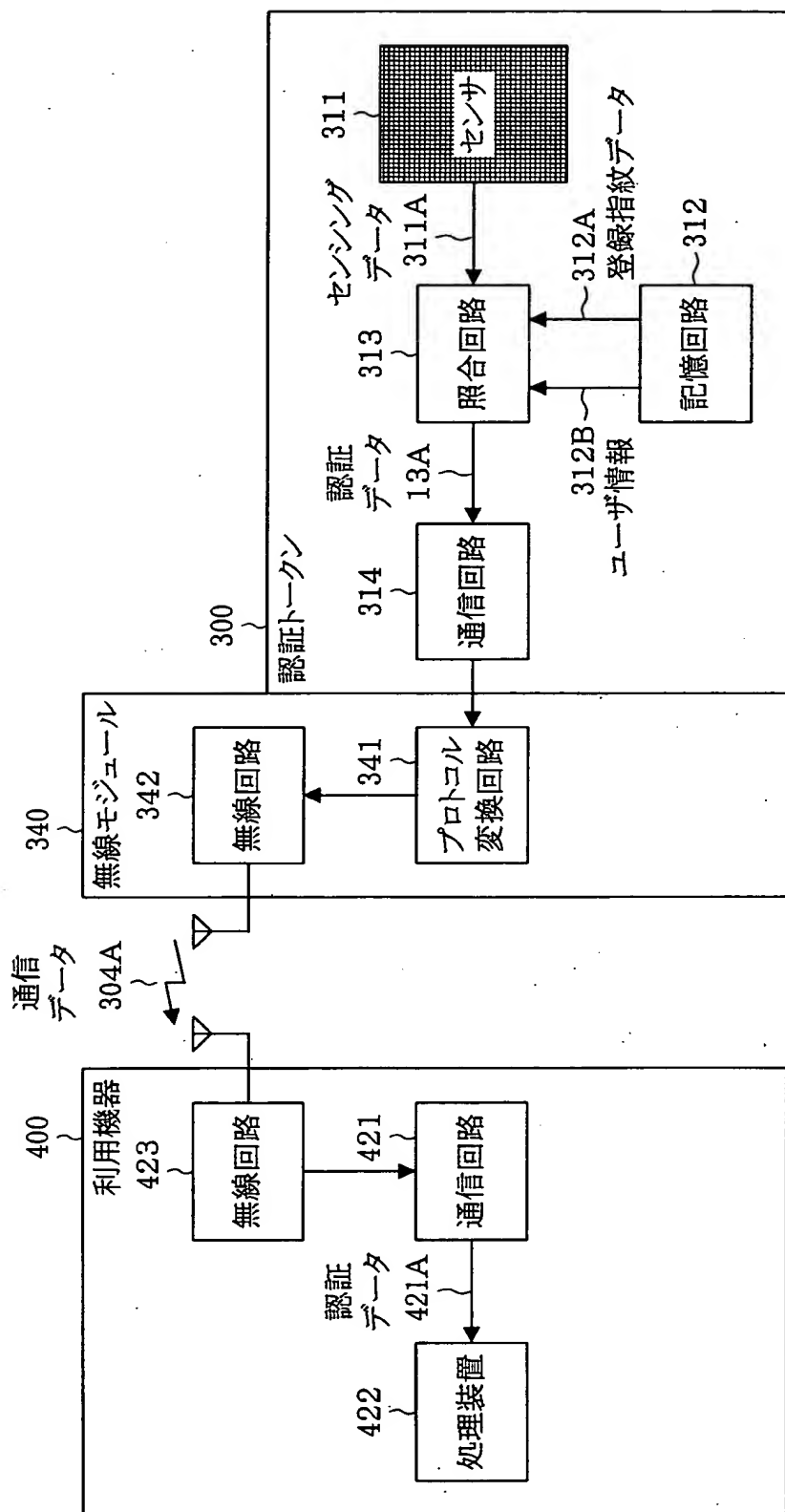
通信データ

ユーザID
パスワード
照合結果
個人情報
⋮

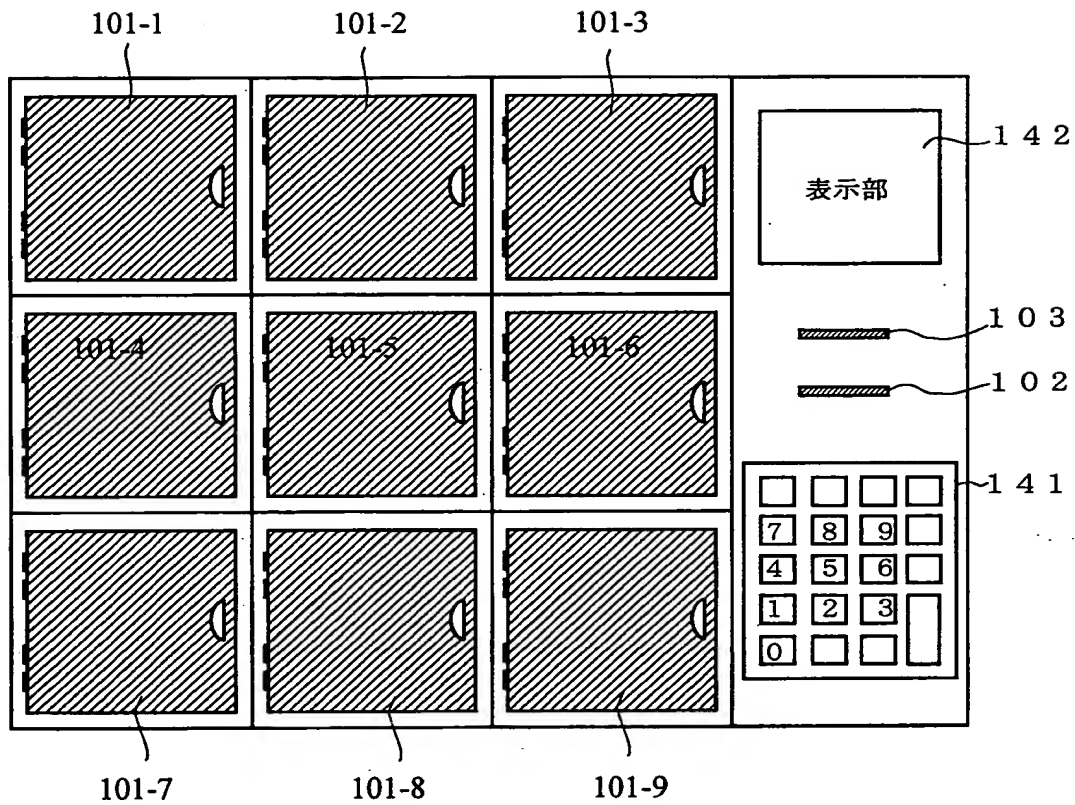
【図 12】



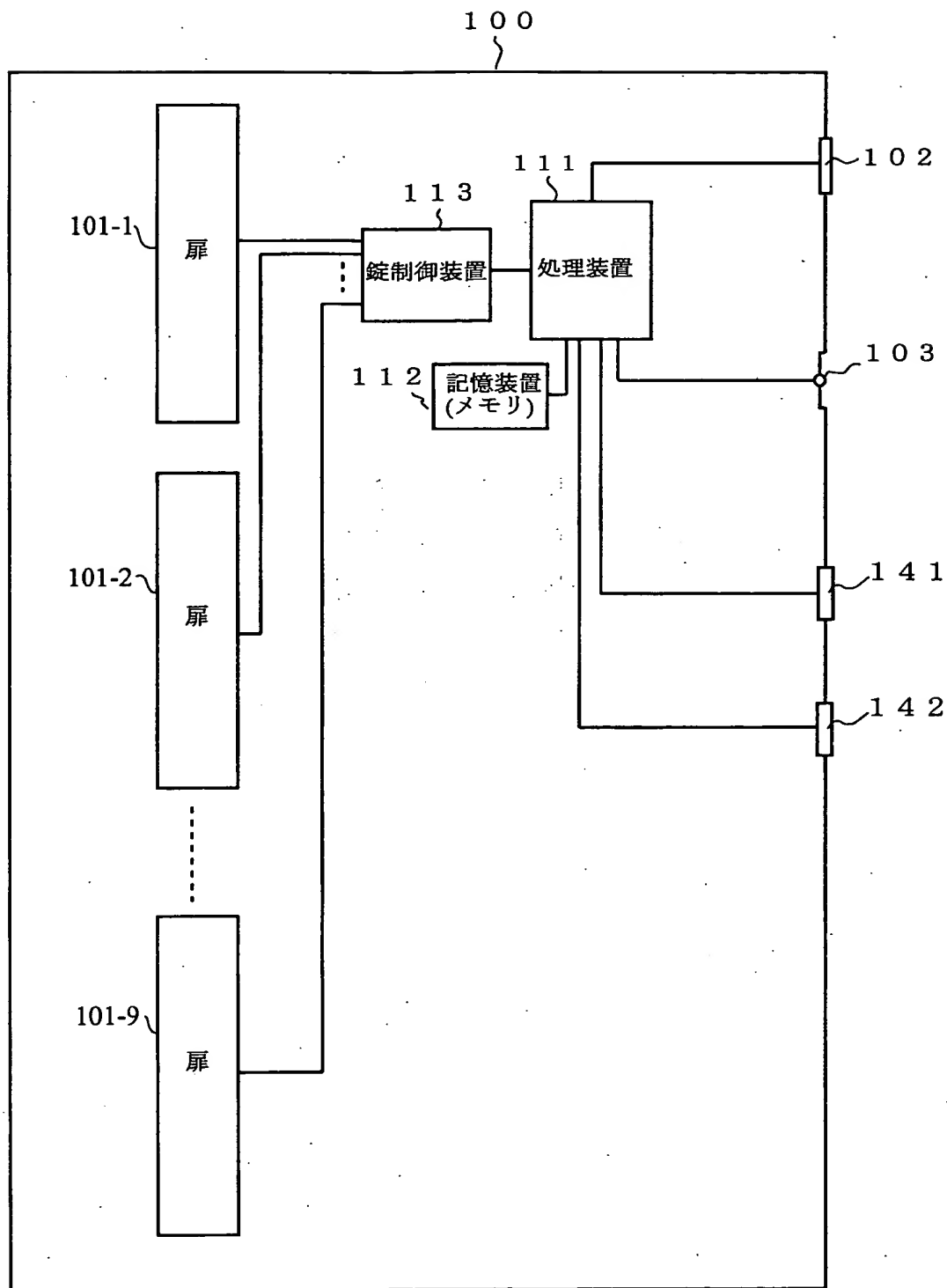
【図 13】



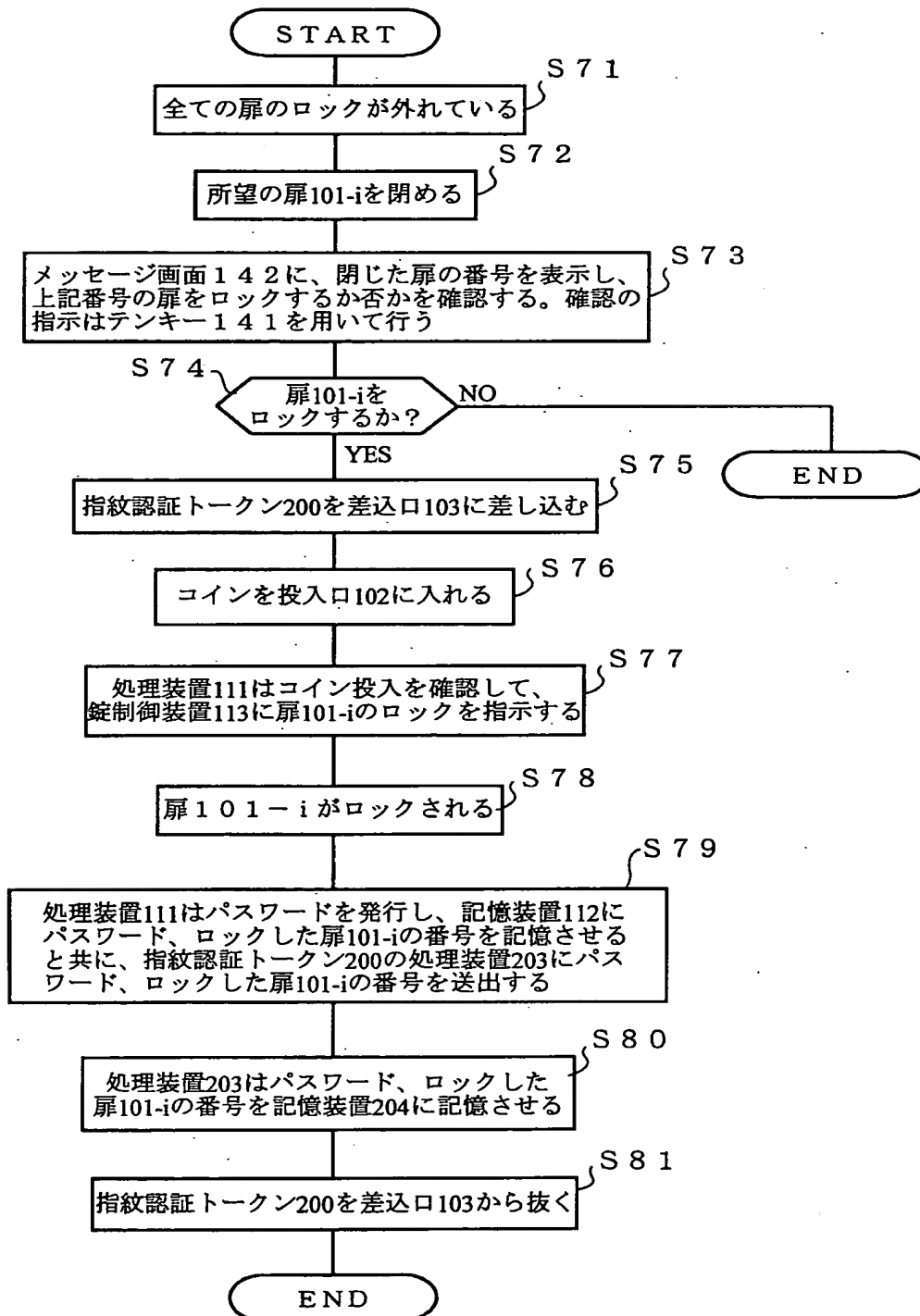
【図 1 4】



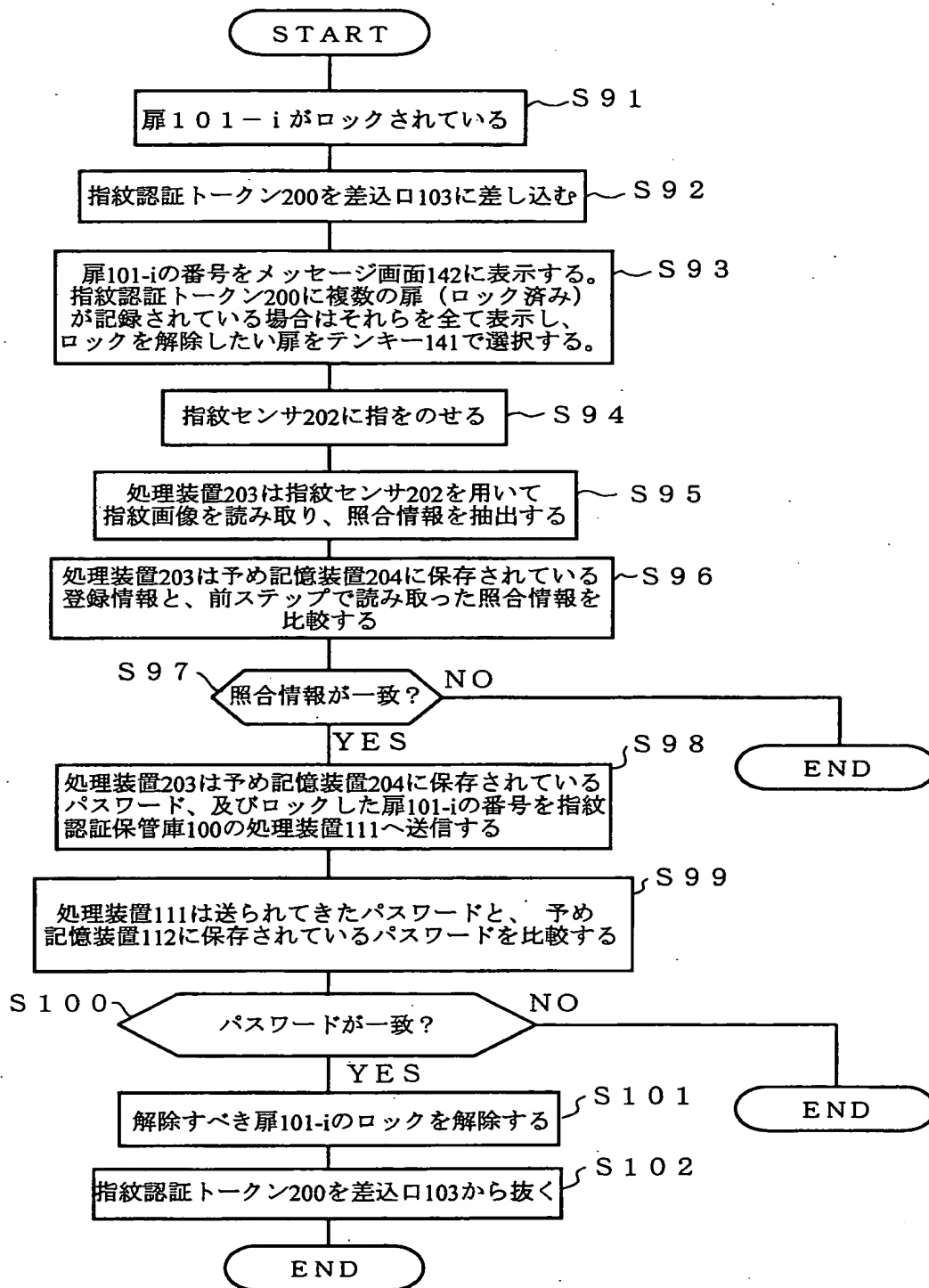
【図 15】



【図 16】



【図 17】





【書類名】 要約書

【要約】

【課題】 コインロッカー等の物品保管庫において、第三者による解錠を阻止しセキュリティを確保する。

【解決手段】 差し込まれた指紋認証トークン200からの出力情報に基づいて扉101のロックを解除可能な指紋認証保管庫100を設けるとともに、指紋認証トークンに利用者の指紋画像を検出する指紋センサ202を設け、かつ指紋認証保管庫に、扉のロック及びロック解除を行う錠制御装置113と、利用者を識別する識別情報を記憶する記憶装置112と、処理装置111とを設け、処理装置は指紋センサの検出に基づき指紋認証トークンから出力される出力情報と記憶装置の記憶情報との一致に基づき錠制御装置を制御し扉のロックを解除する。

【選択図】 図 8

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社